Universität Leipzig
Fakultät für Mathematik und Informatik
Institut für Informatik

Methoden zur Datenaquise für Patientenworkflows

Evaluation von Trackingtechnologien und Simulation eines RFID basierten Erfassungssystems

Diplomarbeit

Leipzig im Dezember 2008

vorgelegt von Frank Eckhardt
Studiengang Medizinische Informatik

Betreuer: Dr. Oliver Burgert
Innovation Center Computer Assisted Surgery (ICCAS)
Gutachter: Prof. Dr. Albert Winter
Institut für Medizinische Informatik, Statistik und Epidemiologie

Inhaltsverzeichnis

Tabellenverzeichnis 6

Abbildungsverzeichnis 7

1. Einleitung 8

1.1. Gegenstand und Motivation . . . 8

1.1.1. Gegenstand . . . 8

1.1.2. Problematik . . . 9

1.1.3. Motivation . . . 10

1.2. Problemstellung und Zielsetzung . . . 11

1.3. Ziel der Simulation . . . 11

1.4. Aufbau der Arbeit . . . 12

2. Theoretische Grundlagen 14

2.1. RFID . . . 14

2.2. XML . . . 19

2.3. EPCglobal und der EPC . . . 20

2.4. ISO und EHIBCC . . . 22

2.5. RFID Anywhere . . . 23

2.5.1. RFID Anywhere Business Module . . . 26

3. Überblick und Bewertung vorhandener Trackingsysteme 28

3.1. Beispiele für verschiedene Lösungen . . . 29

3.1.1. Beispielrechnung für ein typisches Krankenhaus durch Cisco Systems 29

3.1.2. Aus dem Informationsforum RFID . . . 31
3.1.3. Taipei Medical University Hospital . . . 32
3.1.4. Harvard hybrid system . . . 35
3.2. Zusammenfassung . . . 36

4. Machbarkeitsanalyse 38
4.1. Die technischen Anforderungen . . . 38
4.1.1. Mindestanforderungen . . . 38
4.1.2. Probleme durch den Einsatz von RFID auf Medizintechnik . . . 41
4.1.3. Einschätzung . . . 42
4.2. Standards zur RFID-Tag Kennzeichnung . . . 43
4.2.1. EPC Tag . . . 44
4.2.1.1. Kodierung des EPC . . . 46
4.2.1.2. EPC Beispiel . . . 46
4.2.1.3. EPC Global Standards für den Gesundheitsbereich . . . 48
4.2.2. eHIBC Tag . . . 49
4.2.2.1. eHIBC Klassen . . . 50
4.2.2.2. Kodierung des eHIBC . . . 51
4.2.2.3. Speicherformat auf RFID-Tags . . . 52
4.2.2.4. Beispiele für den eHIBC . . . 52
4.2.3. Kompatibilität zwischen EPC und eHIBC . . . 54
4.2.4. Einschätzung der Standardisierung . . . 55
4.3. Datenschutz . . . 56
4.3.1. Vorschriften und Gesetze . . . 57
4.3.1.1. Recht auf informationelle Selbstbestimmung . . . 57
4.3.1.2. Bundesdatenschutzgesetz . . . 57
4.3.1.3. Das Verbot mit Erlaubnisvorbehalt . . . 58
4.3.1.4. Transparenz . . . 59
4.3.1.5. Zweckbindung . . . 60
4.3.1.6. Erforderlichkeit . . . 60

4.3.1.7. Datensparsamkeit 61
4.3.1.8. Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder 61
4.3.2. Maßnahmen zur Sicherung der Datenschutzes 62
4.3.3. Einschätzung 64
4.4. Datensicherheit 65
4.4.1. Gefahren 65
4.4.1.1. Gefahren bei der Übertragung 66
4.4.1.2. Gefahren für RFID-Tags 67
4.4.1.3. Gefahren für Lesegeräte 68
4.4.2. Sicherheitsmaßnahmen 68
4.4.3. Einschätzung 71

5. Simulation eines RFID-Trackingsystems 73
5.1. Aufbau und Planung 73
5.1.1. Räumliche Aufteilung und Anordnung der Lesegeräte 74
5.1.2. Simulationsdaten 76
5.1.2.1. Vorbereitung der Simulationsdaten 76
5.1.2.2. Kodierung der Tags für die Simulation 77
5.1.2.3. Umsetzen im Simulator Data Editor 78
5.1.2.4. Einbinden in RFID Anywhere 80
5.2. Umsetzung der Simulation 80
5.2.1. Implementierung des Business Moduls 80
5.2.1.1. Funktionsweise 82
5.2.2. Das Java Demo GUI 85
5.2.3. Optionen zur Datenverarbeitung und Speicherung 88
5.3. Auswertung 89

6. Zusammenfassung 91

7. Ausblick 93

Literaturverzeichnis 94

A. XML Beispielaufbau 98

B. EPC Headers 99

C. Kodierung der Simulations-Tag-IDs 103

D. Schema der Workflow-Struktur 104

E. Dokumentation und Installation der Simulation 106

Glossar 110

Erklärung 112

Tabellenverzeichnis

2.1. RFID-Frequenzeigenschaften 16

3.1. Kostenersparnis bei besserer Nutzung von Infusionspumpen 30
3.2. Gewinn durch Zeitoptimierung 31

4.1. EPC SGTIN-96 Bit Verteilung 47
4.2. Beispiel für SGTIN-96 Kodierung 47
4.3. Übersicht zu RFID bezogenen ISO-Standards 50
4.4. Übliche DI's unter ISO/IEC 15459 52
4.5. Aufbau eines eHIBC-I Tags 53
4.6. Aufbau eines zusammengesetzten Tags 53
4.7. Übersicht zur Kompatibilität des eHIBC zum EPC 55

B.1. Electronic Product Code Header 101
B.2. Angaben für das Teilungsfeld im EPC Header 102

C.1. Übersicht der verwendeten RFID-Tag IDs 103

Abbildungsverzeichnis

2.1. Übersicht über die genutzten RFID-Frequenzen 15
2.2. Bild eines passiven HF RFID-Transponders 17
2.3. schematischer Aufbau eines passiven RFID-Transponders 17
2.4. schematische Darstellung der magnetischen Induktion 18
2.5. schematische Darstellung der elektromagnetische Induktion 19
2.6. EPC Terminologie 21
2.7. Abbildung der Struktur der RFID Anywhere Architektur 24

4.1. schematischer Aufbau eines RFID Gen 2 Tag 44
4.2. allgemeine Struktur des eHIBC Codes 51
4.3. Angriffsarten 66

5.1. Skizze des Raumplanes der Simulation 74
5.2. Zeitverlauf der simulierten RFID-Tags 77
5.3. Screenshot der Simulationsdatei für das Lesegerät E im RFID Simulator Data Editor 79
5.4. Screenshot der Administratorkonsole 81
5.5. Sequenzdiagramm des RFID Anywhere Business Moduls für die Simulation 83
5.6. Sequenzdiagramm der Java Demo GUI 86

D.1. grafisches Schema der Workflow Struktur - Teil 1 104
D.2. grafisches Schema der Workflow Struktur - Teil 2 105

E.1. Einstellungen für die Optionen des Business Moduls „firstSim“ 108

1. Einleitung

> Was sich die Menschen einbilden, ist gleichgültig. Lediglich die Erkenntnis der Dinge ist von Bedeutung. Sie allein macht unsere Schlussfolgerungen wertvoll.
>
> *John Locke (1, 218), Über den menschlichen Verstand*

1.1. Gegenstand und Motivation

1.1.1. Gegenstand

Etwas Ähnliches wie John Locke hatten wohl auch die Verantwortlichen in einem großen Leipziger Krankenhaus erkannt, als dort beschlossen wurde, genau zu untersuchen wie bestimmte Patienten das eigene Haus nach der Aufnahme durchlaufen. Man glaubte zwar ungefähr zu wissen was vor sich ginge, aber ausreichend gesicherte Informationen hatte niemand. Daher wurde begonnen, sich mit dem Gedanken zu beschäftigen, Informationen über den Verbleib der eigenen Patienten innerhalb des Krankenhauses oder über bestimmte Teile ihrer Behandlung zu erlangen. Aus diesem Grund wurden mehrere Patienten persönlich begleitet, um ihre jeweiligen so genannten Patientenpfade zu ermitteln. Diese erste Untersuchung führte neben einigen wenigen Informationen zu der Erkenntnis, dass die Beobachtung einzelner Patienten wenig effektiv ist. Denn für jeden zu begleitenden Patienten wäre eine aufnehmende Person nötig. Der Aufwand einen Patienten Schritt für Schritt zu verfolgen, steht aber in diesem Fall in keinem Verhältnis zur Menge der gewonnen Daten. Diese Erkenntnis resultierte in der Überlegung, eine höhere Zahl an

Individuen ohne den hohen personellen Aufwand zu erfassen. Als eine Möglichkeit wurde dabei die Verfolgung mittels der Radiofrequenz-Identifikation in Betracht gezogen. Während die drahtlose Identifizierung in der Industrie bereits erfolgreich zum Einsatz kommt, ist die Portierung der bestehenden Technik in den Gesundheitsbereich bisher kaum erfolgt.

Ausschlaggebend für das aktuelle Bemühen um mehr Informationen ist das Streben nach Verbesserung. Seit der Einführung der DRG im Januar 2003, als Werkzeug zur Vergütung im deutschen Gesundheitssystem, sind Krankenhäuser aufgefordert die Behandlung ihrer Patienten zu optimieren. Bevor Abläufe aber optimiert werden können, ist es nötig sie zu erfassen [3, S. 77]. Die dazu notwendigen Werkzeuge für die Aufnahme und Messung von Prozessen, sind verfügbar und einsatzbereit. Zum Beispiel werden so bereits chirurgische Abläufe als Workflow festgehalten [10] und anschließend analysiert. Die Verfolgung oder das Tracking von Patienten in einem Krankenhaus mittels RFID, wäre so nur eine Erweiterung der Möglichkeiten der Workflowerfassung.

1.1.2. Problematik

Das eigentliche Problem besteht darin, dass es nur wenige gesicherte Informationen über genaue Zeiten und Abfolgen der einzelnen Stationen bei der Behandlung der Patienten gibt. Die Patienten durchlaufen die verschiedensten Bereiche des Krankenhauses im Zuge ihrer Untersuchungen. Die Abteilungen arbeiten zwar zusammen, doch jede von ihnen ist für sich unabhängig. Diese Aufteilung macht es den betreffenden Mitarbeitern schwer, einen Überblick über die Gesamtsituation bei der Patientenversorgung zu erhalten. Die Verantwortlichen des erwähnten Krankenhauses suchten deswegen einen Weg, um einen ganzheitlichen Blick auf den Patienten zu erlangen. Der Hauptgrund dafür ist der Druck Effizient und Kostendeckend zu arbeiten. Untersuchungen zu den oben genannten Reformen besagen, dass in Zukunft rund ein Drittel aller Kliniken nicht wirtschaftlich arbeiten werden können [35]. Überflüssige Behandlungen und unnötige Wartezeiten werden seit der Umstellung auf die DRG-Fallpauschalen nicht mehr durch Tagessätze aufgefangen.

Die Krankenhäuser sind demnach bestrebt ihre eigenen Abläufe zu verbessern. Denn eine schnellere Genesung bedeutet eine frühere Entlassung.

Ein Konzept zur Umsetzung des Wunsches nach Beobachtung existierte in diesem Fall nicht. Der Versuch einzelne Patienten zu begleiten war ein Test, der sich als nicht praktikabel herausstellte. Auch wenn die Aufnahmen Softwaregestützt mit Hilfe eines Workfloweditors [11] durchgeführt wurden, ist diese Form zu beschränkt was die Zahl der aufzunehmenden Personen anbelangt. Die Idee RFID-Technik einzusetzen scheint eine Lösung dafür zu sein. Allerdings existieren im Gesundheitsbereich wenig Erfahrungen mit der Technik, da die Radiofrequenz-Identifikation bisher hauptsächlich im Bereich der Inventarverwaltung verwendet wurde. Auch sollen in diesem Szenario Personen beobachtet werden, was im Gegensatz zur Warenidentifikation Datenschutzbedenken aufwirft. Es gilt dahingehend zu bedenken, dass im Gesundheitswesen andere Ansprüche an Sicherheit und Vertraulichkeit gestellt werden.

1.1.3. Motivation

Die Entwicklung eines RFID basierten Trackingsystems für Patienten kann verschiedene Vorteile generieren. Für die Krankenhäuser bietet sie z.B. die Möglichkeit ihre eigenen Abläufe und Prozesse in Form von Patientenpfaden zu erheben und sie dann zu analysieren. Mit dieser Methode der Datenaquise lassen sich mehr Informationen generieren als bei einer Beobachtung oder Befragung der Patienten alleine. Untersuchungen wie die erwähnte Studie vom McKinsey zeigen, dass es in Zukunft notwendig sein wird, in kürzerer Zeit, mit weniger Aufwand, mehr Patienten zu behandeln. Dafür wird es an einigen Stellen nötig sein, die Organisation und die Behandlung der Patienten zu verbessern.

Gleichzeitig steht auch die Patientenzufriedenheit als Punkt zur Kontrolle an. Durch die Bemühung die Qualität und die Zufriedenheit weiter zu gewährleisten oder auch zu verbessern, wird versucht eine Abwanderung der benötigten Patienten an andere Kliniken zu vermeiden. Später wäre ein mögliches RFID-Netzwerk dabei nicht nur Mittel zur Erfassung der Daten, sondern auch zur Kontrolle der gesetzten Qualitätsmaßstäbe.

1.2. Problemstellung und Zielsetzung

- Es ist nicht bekannt, ob einsatzfähige Systeme zur automatischen Lokalisierung und Erfassung von Patienten in einem Krankenhaus existieren. Daher soll geprüft werden, ob es Lösungen gibt, die diese Aufgabe lösen können.
- Es gibt eine Vielzahl von RFID Hardware. Es stellt sich die Frage, ob es bestimmte Anforderungen für den Einsatz im Krankenhaus gibt und ob es technisch möglich ist das Tracking der Patienten umzusetzen. Deswegen wird unter Berücksichtigung eines festgelegten Szenarios überprüft, welche technischen Anforderungen an ein RFID-Trackingsystem gestellt werden könnten.
- Wie bereits erwähnt, können in einem Krankenhaus sensible Daten erhoben werden. Es soll ermittelt werden, welche Bestimmungen und Vorschriften für den Datenschutz und die Sicherheit der Informationen vom Betreiber des RFID-Netzwerkes beachtet werden müssen.
- Kann ein solches Vorhaben im Vorfeld geplant und getestet werden ohne die komplette Infrastruktur dafür zu besitzen? Das Ziel ist es, eine Simulation für ein bestimmtes Szenario zu entwickeln und auf seinen Nutzen hin zu überprüfen. Genaueres dazu entnehmen Sie dem den folgenden Abschnitt 1.3.

1.3. Ziel der Simulation

Die Implementierung im Rahmen dieser Arbeit hat das Ziel, das RFID-Framework „RFID Anywhere“ von Sybase zu testen und die Weiterverwendung der darin erzeugten Daten zu prüfen. Wie können diese erhoben, verarbeitet, angezeigt oder versendet werden? Der reale Aufbau eines RFID-Netzwerkes sollte dabei vermieden werden. Stattdessen soll eine Simulation erstellt werden. Die Gründe dafür sind verschieden. Zum einen kann die Möglichkeit getestet werden, ein RFID-Netzwerk simuliert zu erstellen. Damit wäre es möglich den Funktionsumfang eines geplanten Trackingsystems bereits im Vorfeld zu

überprüfen. Die Software zur Weiterverarbeitung der Daten könnte damit, noch vor oder während des Aufbaus des eigentlichen Netzwerkes implementiert und gestestet werden. Ein Test mit realer Hardware, beansprucht in diesem Umfang Platz und hätte Investitionen in Lesegeräte, RFID-Tags und Netzwerktechnik nötig gemacht. Zusätzlich wäre ein nicht unerheblicher organisatorischer Aufwand nötig geeignete Daten zu generieren, da mehrere Personen oder Träger von RFID-Tags sich durch das simulierte Raumsystem bewegen müssten.

So wird ein Personentrackingsystem implementiert, dass Bewegungen von Personen simuliert. Dies können Patienten und Mitarbeiter des Krankenhauses sein, genauso wie medizinische Geräte und andere Dinge, die mit RFID-Tags versehen wurden. Die Daten dazu werden durch die verfügbaren Funktionen des Frameworks geliefert und durch ein selbst erstelltes Business Modul verarbeitet. Die daraus gewonnenen Informationen werden in Echtzeit durch eine Demoapplikation angezeigt und durch diese an ein Workflow-Aufnahmesystem [11] gesendet. Damit wird eine Möglichkeit zur Verwendung der Daten ebenfalls getestet.

Zusammenfassend soll ein Modell entwickelt werden, dass Daten generiert. Dazu wird ein simuliertes System aus verschiedenen Räumen beschrieben und mit virtuellen Lesegeräten versehen. Durch dieses Modells werden Simulationsdaten erstellt, die durch die Lesegeräte generiert werden. Die Informationen zu den simulierten Personen sollen angezeigt werden, um die Positionsbestimmung aller im System befindlichen Personen live zu demonstrieren. Gleichzeitig dazu, werden die Informationen zur Datenverarbeitung weiterversandt. Die Anbindung an das genannte Workflowerfassungssystem, wird im Rahmen der Demoapplikation ebenfalls getestet.

1.4. Aufbau der Arbeit

Um die Voraussetzungen für die anschließende Untersuchung und die Technik der Implementierung zu schaffen, beginnt die Arbeit mit der Übersicht über die technischen

und theoretischen Grundlagen in Kapitel 2. Nach der Einführung folgt die Suche nach bereits existierenden Lösungen in Kapitel 3. Hier werden verschiedene Lösungsansätze oder Umsetzungen vom RFID-Tracking in Krankenhäusern oder im Gesundheitssystem betrachtet und bewertet. Das Kapitel 4 beinhaltet die Untersuchung auf die generelle, technische und rechtliche Machbarkeit. In der jüngsten Vergangenheit standen Themen wie automatische Überwachung, elektronische Verfolgung und Tracking in keinem guten Licht[1]. So haben die bisher geführten Diskussionen zur Erweiterung der deutschen Reisepässe durch RFID-Chips mit darauf gespeicherten biometrischen Daten oder zur Vorratsdatenspeicherung, das Vertrauen in die Sicherheit durch die neue Technik nicht verbessert [20, Seite 149 ff].

Den Grundlagen zum Schutz persönlicher Daten und der Datensicherheit soll in dieser Arbeit ebenso Beachtung geschenkt werden, wie den technischen Aspekten. Denn schon Mark Weiser[2], der sich bereits 1991 mit den Gefahren der rechnergestützten Informationsverarbeitung im Alltag befasste, erkannte das Problem unsichtbarer allgegenwärtiger Erfassung. Er prägte dafür den Namen „Ubiquitous Computing“ in dem Aufsatz „The Computer for the Twenty-First Century“ [43]. Es gilt also auch herauszufinden, in wie weit das deutsche Datenschutzgesetz anzuwenden ist und geltende Gesetze beachtet werden müssten. Sollten sich dann zu den Bedenken der Öffentlichkeit [7, Kapitel 10.2.5.][5, Seite 5 f], rechtliche Probleme einstellen, wäre das Vorhaben in der Realität nicht umzusetzen. Es ist zu zeigen, welche Dinge bei der Umsetzung beachtet werden sollten, um nicht in technische oder rechtliche Probleme zu geraten. Zum Abschluss und um den Aufwand beziehungsweise das Konzept eines RFID-Trackingsystems zu verdeutlichen, wird die Simulation eines einfachen RFID-Aufbaus implementiert. Das Kapitel 5 setzt sich in vollem Umfang damit auseinander. Zum Abschluss erfolgt in Kapitel 6 die Zusammenfassung der erarbeiteten Ergebnisse.

Um die Simulation selbst zu testen befindet sich im Anhang E die Dokumentation und die Anleitung zur Installation. Die Software selber befindet sich auf der beigelegten CD.

[1] http://www.boycottbenetton.com/
[2] http://sandbox.parc.com/weiser/

2. Theoretische Grundlagen

In diesem Kapitel werden die wichtigsten Grundlagen beschrieben, die sowohl für den theoretischen Teil als auch die Umsetzung der Simulation notwendig sind. Sie beinhalten eine Übersicht zur Radiofrequenz-Identifikation (RFID), dem Speicherformat XML und zum Tracking. Es werden die Standardisierungsorganisationen EPCglobal und ISO/E-HIBCC vorgestellt. Der letzte Punkt ist die Beschreibung der in der Implementierung verwendeten Simulationsumgebung namens RFID Anywhere.

2.1. RFID - Radio Frequency Identification

RFID ist die Abkürzung für Radio Frequency Identification und wird mit Radiofrequenz-Identifikation übersetzt. RFID steht für das drahtlose Auslesen von Daten mit Hilfe von elektromagnetischen Wellen, die auf einem RFID-Tag gespeichert sind. Durch verwenden von Funkwellen, entfällt der bisher nötig gewesene direkte Kontakt zwischen Lesegerät und Datenträger. Im Gegensatz dazu sind Strich- oder Barcodes von einer direkten visuellen Sichtlinie abhängig. Die Übertragung per Funk benötigt weder eine direkte physikalische Verbindung noch eine Sichtlinie oder einen uneingeschränkten Zugang zum Datenträger.

Die Sendefrequenzen mit denen RFID-Systeme arbeiten sind weltweit geregelt. Sie bewegen sich in den lizenzfreien ISM-Bändern (Industrial-Sientific-Medical), die international für besagte industrielle, wissenschaftliche und medizinische Zwecke freigehalten werden. Innerhalb dieser Frequenzen sind die Bänder von 135 kHz bis 900 MHz fest-

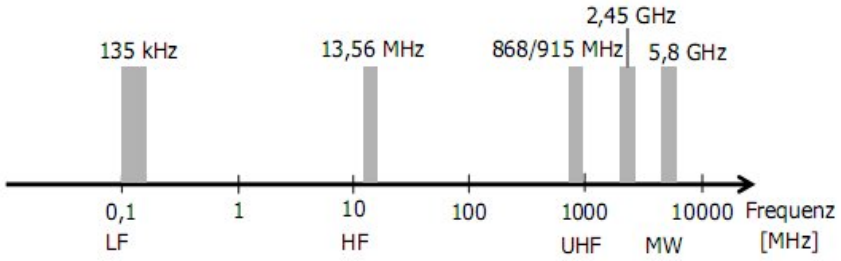


Abbildung 2.1.: Übersicht über die genutzten RFID-Frequenzen [33]

gelegt worden (siehe Abb. 2.1). Die Frequenzen um 135 KHz sind für Niederfrequenz-Transponder (LF), die Hochfrequenten-Transponder (HF) arbeiten bei 13,56 MHz. Die Ultrahochfrequenten-Transponder (UHF) arbeiten bei Frequenzen um 900 MHz. Je nach Region werden sie auf unterschiedlichen Frequenzen betrieben. 433 MHz und 868 MHz gelten in Europa, 915 MHz in den USA und 950 MHz in Japan [33].

Ein RFID-System besteht aus zwei Hauptkomponenten. Dem Lesegerät und dem RFID-Transponder bzw. RFID-Tag. Ein Transponder setzt sich aus einem Transmitter und einem Responder zusammen [18]. Er nimmt empfangene Signale auf und beantwortet diese automatisch. Die Transponder können dabei passiv oder aktiv mit Strom versorgt sein. Passiv bedeutet, dass der Transponder die benötigte Energie, zum Empfangen, Verarbeiten und Senden von Daten, ausschließlich aus dem elektromagnetischen Feld des Lesegeräts zieht [33]. Passive Transponder bringen sonst keine eigene Stromversorgung mit. Aktive Transponder besitzen dagegen eine eigene Energiequelle, wodurch sich die maximale Sendereichweite erhöht. Auch die Möglichkeiten der Datenverarbeitung und Datenspeicherung auf den RFID-Tags selbst sind vielfältiger als bei passiven Tags. In der Regel wird im Zusammenhang mit RFID von passiven Transpondern (Siehe Abb. 2.2) gesprochen. Durch den Verzicht auf eine eigene Stromquelle, können die RFID-Tags sowohl sehr klein als auch sehr günstig produziert werden.

Die passiven Transponder bestehen in ihrer einfachsten Bauweise hauptsächlich aus den in Abbildung 2.3 gezeigten Komponenten.

Er besteht hauptsächlich aus einer Antenne, einem Kondensator und einem Chip. In

	LF 0 - 135 kHz	HF 3 - 30 MHz	UHF 0,2 - 2 GHz	MW > 2 Ghz
Art der Kopplung	Induktive Kopplung (arbeitet im Nahfeld)		Elektromagnetische Kopplung (arbeitet im Fernfeld)	
Typische Frequenz	134,2 kHz	13,56 MHz	868 MHz (EU) 915 MHz (USA)	2,45 GHz 5,8 GHz
Typische Lesereichweite	< 1,5 m	< 1,0 m	Passive Transponder: < 3 m (EU bei 0,4 W) ca. 3-5 m (EU bei 2 W, geplant) ca. 5-7 m (US bei 4 W)	
Negative Umgebungseinflüsse	– Abschirmung – leitfähige Materialien (z.B. Metall)		– Abschirmung – Absorption, Reflexion, Brechung	
Einflüsse der Transponder untereinander	Antennen-Verstimmung bei engliegenden Transpondern		Verzerrung der Funkmuster aufgrund von Antennenkopplung	

Tabelle 2.1.: Überblick der wichtigsten Eigenschaft von RFID-Frequenzen [33, Seite 10]

der Antenne wird durch das elektromagnetische Feld des Lesegeräts ein Strom induziert. Dieser wird gleichgerichtet und im Kondensator gespeichert. Mit der aufgenommenen Energie wird der Chip versorgt. Eine weitere Besonderheit ist, dass die Transponder zur Übermittlung der Daten kein eigenes Feld aussenden, sondern das Sendefeld des Lesegeräts durch Feldschwächung oder Reflexion modulieren [33, S. 6 ff]. Die durch den Transponder verursachten Veränderungen werden durch das Lesegerät registriert und ausgewertet.

Allerdings unterscheidet sich nach bestimmten Frequenzen die Art und Weise wie in der Antenne Strom induziert wird. Die Nieder- (LF) und Hochfrequenten (HF) Bänder induzieren Strom über ein magnetisches Wechselfeld in einer Antenne, die wie eine Spule aufgebaut ist. In der Abbildung 2.4 ist die grundlegende Funktionsweise der ma-

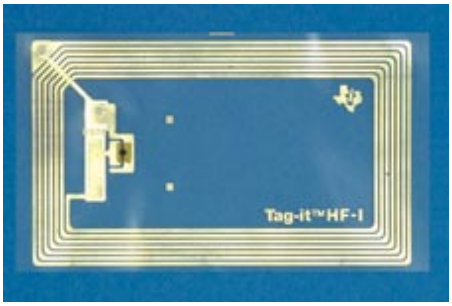


Abbildung 2.2.: Bild eines passiven HF RFID-Transponders von Texas Instruments [40]

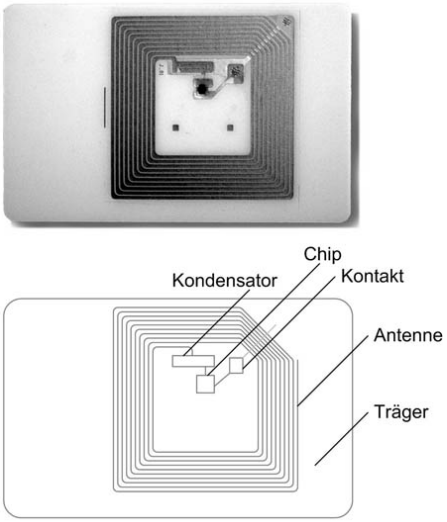


Abbildung 2.3.: schematischer Aufbau eines passiven RFID-Transponders [38]

gnetischen Induktion. Die Ultrahochfrequenten (UHF) und Mikrowellenbänder (MW) übertragen Energie mit Hilfe einer elektromagnetischen Welle, die von Antennen mit Dipolarmen aufgefangen werden. Der Grund dafür liegt in der Entfernung in der die Tags ausgelesen werden können und den unterschiedlichen Wellenlängen der dafür genutzten Frequenzbänder.

Der aufgeladene Kondensator liefert bei der magnetischen Induktion oder Kopplung den benötigten Strom, um die vom Lesegerät empfangenen Befehle zu verarbeiten und die Antwort zu senden. Im einfachsten Fall enthält der Tag lediglich eine Tag-ID, welche er an das Lesegerät zurück sendet. Die Übertragung selbst wird codiert und in Änderungen

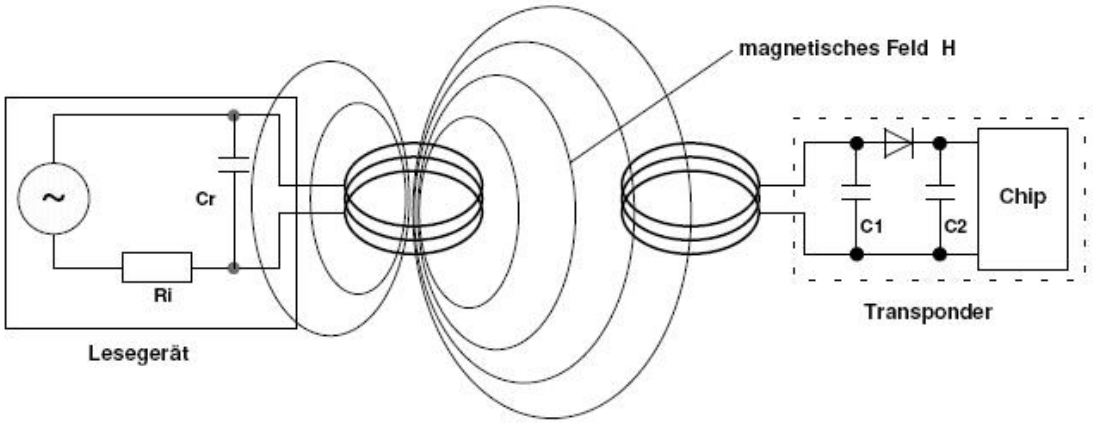


Abbildung 2.4.: schematische Darstellung der magnetischen Induktion [18]

eines Widerstandes umgesetzt. Dabei ändert sich die Induktivität des Transponders, was zu kleinen Spannungsänderungen führt [33]. Das Lesegerät misst diese und decodiert die so übertragenen modulierten Daten. Bei dieser Art der Datenübertragung ist die Reichweite allerdings beschränkt. Die Feldstärke eines Magnetfeldes nimmt im Nahfeld proportional zur dritten Potenz der Entfernung ab.

$$E \approx \frac{1}{r^3} \tag{2.1}$$

Dafür besitzt das Nahfeld die höhere Feldstärke, wodurch mehr Strom induziert und auf eine zusätzliche Energiequelle weitgehend verzichtet werden kann. Grundsätzlich ist die Feldstärke aber von der Leistung des Lesegeräts, der Sendefrequenz und dem Durchmesser der Spule des Lesegerätes abhängig. So entspricht bei einem passiven Transponder im Scheckkartenformat die maximale Reichweite des Lesegeräts ungefähr seinem Spulendurchmesser. Den Nachteil der geringen Reichweite wiegt der Vorteil auf, dass die LF- und HF-Bänder weniger anfällig für Störungen durch Metalle und Flüssigkeiten sind.

Die elektromagnetische Induktion, in Abbildung 2.5 dargestellt, liefert genau wie die magnetische Induktion eine Wechselspannung, die gleichgerichtet und durch einen Kondensator gespeichert wird. Die hier verwendeten höheren Frequenzen bewirken eine höhere maximale Reichweite als bei der magnetischen Induktion. Die magnetische Kopplung funktioniert nur im oben genannten Nahfeld, während im UHF und MW Bereich im

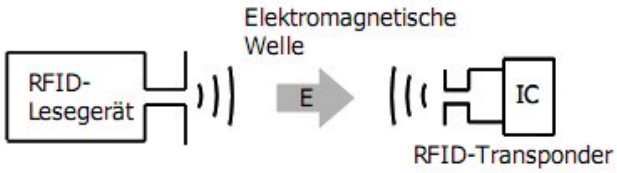


Abbildung 2.5.: schematische Darstellung der elektromagnetischen Induktion [33]

elektromagnetischen Fernfeld noch Energie induziert wird. Als Fernfeld wird ein elektromagnetische Feld bezeichnet, das mehr als 3 Wellenlängen vom Sender entfernt ist. Da im Fernfeld die Energie nur proportional zum Quadrat der Entfernung abnimmt,

$$E \approx \frac{1}{r^2} \tag{2.2}$$

ist die Reichweite bei passiven Transpondern zwar begrenzt, baut aber nicht so schnell ab wie im Nahfeld. Bei passiven Transpondern sind 5 - 7m möglich, bei aktiven Transponder Reichweiten zwischen 15 - 100m [33]. Die Übertragung der Daten erfolgt ebenfalls indem sich ein Widerstand an- und abschaltet und so ein Signal codiert. Hier wird jedoch die ankommende Welle reflektiert und dann verändert. So wird ein codiertes Signal erzeugt, das dann vom Lesegerät empfangen, decodiert und ausgewertet werden kann.

2.2. XML - Extensible Markup Language

XML steht als Abkürzung für Extensible Markup Language. Sie ist eine vom World Wide Web Consortium (W3C) herausgegebene Klasse von Datenobjekten, genannt XML-Dokumente [13].

XML wird seit 1996 von einer XML-Arbeitsgruppe entwickelt, die unter der Schirmherrschaft des W3C gegründet wurde. XML soll es als eingeschränkte Version der SGML, der Standard Generalized Markup Language, ermöglichen den Inhalt und die Darstellung von Daten zu trennen. Dafür sind sie aus Speichereinheiten aufgebaut, den Entities, die sich zwar an die vorgegebenen Spezifikationen halten müssen, aber frei wählbar sind im Namen. Dabei ist es auch irrelevant ob dies reine Daten in Form von Text, Grafiken oder

anderen Formen beinhalten. Nur Inhalte in Form von Binärdaten sind per Definition ausgeschlossen.

Zusätzlich wurden 10 Entwurfsziele festgelegt, die im wesentlichen besagen, dass es einfach im Internet zu nutzen, für Menschen lesbar und verständlich, leicht zu erstellen, formal und präzise sein soll. Die genauen Spezifikationen und Ziele, sind in den frei verfügbaren XML-Spezifikationen nachzulesen [13].

Im Anhang A ist ein Beispiel für eine XML Datei angefügt.

2.3. EPCglobal und der Electronic Product Code

Im Zuge der Radio Frequenz Identifikation und den damit verbundenen Plänen einer weltweit eindeutigen Kennzeichnung und Identifikation von Objekten entstand die Non-Profit-Organisation EPCglobal[1]. Sie wurde 2003 von der EAN International und der Uniform Code Council, Inc. gegründet. Diese beiden Organisationen, die unter anderem auch die internationalen Standards für die Barcodes festlegen, unterstützten bereits die Forschung des Auto-ID Centers. Dieses Center hatte die Aufgabe international gültige Standards für Transponder, Lesegeräte und die zugehörigen Informationssysteme zu entwickeln [19]. Nachdem die Forschung in diesem Bereich 2003 planmäßig beendet wurde, gründeten die beiden oben genannten Organisationen die EPCglobal mit dem Ziel, die kommerzielle Umsetzung und Weiterentwicklung der Normen und Standards fortzuführen. Seit 2003 ist die EPCglobal nach eigener Aussage für die Entwicklung von Standards zur „einheitlichen Nutzung der Radio Frequenz Technologie für Identifikationszwecke (RFID) entlang der gesamten Versorgungskette über Länder- und Branchengrenzen hinweg“ [24] verantwortlich.

Der größte Unterschied zu den bisher verwendeten Produktcodes wie dem Barcode ist die Tatsache, dass der Code neben dem Hersteller und Produktnummer, auch eine Seriennummer enthält. Mit diesen Informationen, lassen sich einzelne Objekte individuell

[1] http://www.epcglobal.de/

identifiziert. Dieser Electronic Product Code (EPC) ist damit eine weltweit überschneidungsfreie Ziffernfolge, mit der die eindeutige Identifizierung sichergestellt ist.

Der EPC ist wie in Abbildung 2.6 dargestellt aufgebaut. Der 64 Bit bzw. mittlerweile 96 Bit lange EPC, wurde in 4 Abschnitte eingeteilt. Deren Struktur wurde international vereinbart und ist damit für jeden EPC gültig [17].

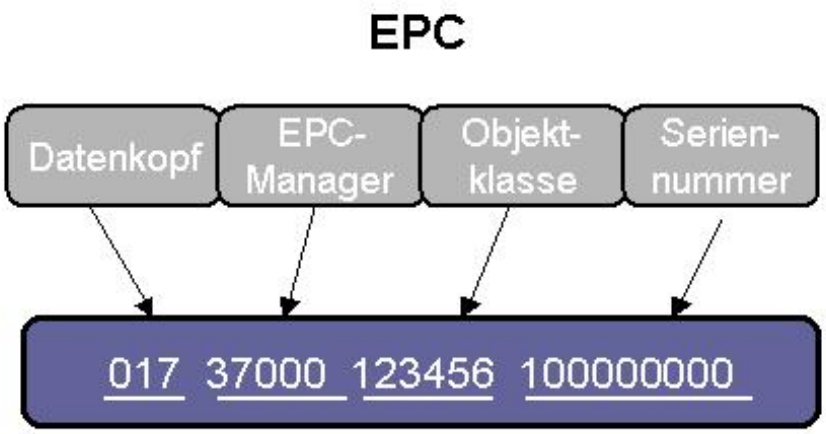


Abbildung 2.6.: EPC Terminology [24]

Der **Datenkopf** oder **Header** steht immer am Anfang der Ziffernfolge. Er legt fest, welcher Typ von EPC vorliegt und mit welcher Codierung der Rest der ID verschlüsselt ist.
Der **EPC-Manager** (**General Manager Number**) stellt die Kennzeichnungsnummer des Nummernbesitzers dar. Dies ist zum Beispiel der Hersteller oder die Firma, welche den EPC verwendet.
Die **Objektklasse** (**Object Class**) bezeichnet den Bereich für Kategorien, Produktgruppen oder andere Einteilungen.
Die **Seriennummer** (**Serial Number**) ist eine eindeutige Seriennummer innerhalb der Objektdomäne.

Dies sind alle Daten die EPC-konform zur Identifizierung gespeichert werden. Neben der Standardisierung der Struktur, werden die Informationen mit denen der EPC ver-

schlüsselt ist, zentral durch die EPCglobal verwaltet. Als wesentliches Merkmal, bietet die Organisation die Möglichkeit an, zu jedem EPC die zugehörigen Daten abzufragen. Die Übertragung der Daten erfolgt über das Internet. Das Konzept des „Internet der Dinge“ stand hier schon zu Zeiten des Auto-ID Labs Pate und bezeichnet die elektronische Vernetzung von Gegenständen des Alltags. Erst durch den weltweiten und allgegenwärtigen Zugriff auf diese Informationen werden die von der EPCglobal beschriebenen Vorteile der RFID-Technologie wie Informationstransparenz, Rückverfolgbarkeit, Zeitvorteile u.a. möglich. Aus diesem Grund beschränkt sich die Entwicklung und Forschung nicht nur auf den EPC, sondern auch auf die Komponenten die nötig sind das weltweit verfügbare Netzwerk zu realisieren [22]. Ein Zeitpunkt für die Inbetriebnahme ist bisher nicht bekannt.

2.4. ISO und EHIBCC

ISO ist die Abkürzung für *International Organization for Standardization*. In diesem Netzwerk aus international arbeitenden Standardisierungseinrichtungen aus 157 Ländern, werden internationale Standards entwickelt und veröffentlicht. Die ISO ist eine unabhängige Einrichtung, die sowohl staatliche als auch private Einrichtungen vereint.

Die EHIBCC, die *European Health Industry Business Communication Council*, ist der nationale Verband der HIBCC[2]. Die HIBCC entwirft und verwaltet Standards für medizinische Barcodes im Gesundheitswesen. Im Gegensatz zum Barcode-Vorgänger des EPC ist die HIBC-Kodierung der HIBCC speziell an die Bedürfnisse des Gesundheitswesen angepasst. Zusätzliche Informationen, wie z.B. ein Verfallsdatum, lassen sich so mit in den Barcode kodieren. Die HIBCC-Standards wurden in den entsprechenden ISO-Standards übernommen. Dazu mehr in Kapitel 4.2.2

[2] http://www.hibcc.org/

2.5. RFID Anywhere

RFID Anywhere ist eine Plattform zur Planung und Umsetzung von RFID-Systemen. Die zu Sybase Inc.[3] gehörende Firma iAnywhere Solutions Inc. bietet ein System an, um die RFID-Hardware, Standards und Protokolle zu simulieren. Sie abstrahiert, die technische Ebene von der Möglichkeit RFID Lösungen zu entwerfen, indem sie Simulations- und Verwaltungsmittel in einer Softwareplattform zusammenfasst [28]. Der Vorteil, sich bei der Entwicklung auf die Business Logik zu konzentrieren und die Hardwarearchitektur später und unabhängig zu planen, fördert die Entwicklung von RFID-Systemen. Da es zur Realisierung der Simulation keine Möglichkeit gab, ein Krankenhaus mit einem kompletten RFID-Netzwerk und der damit verbundenen nötigen lückenlosen Überwachung als Versuchsort zu nutzen, hätte zum Testen ein Demonstrationssystem installieren werden müssen. Der technische Aufwand für ein RFID-Trackingsystem in einer hinreichenden Größe ist jedoch relativ hoch. Für den Test hätten mehrere Lesegeräte beschafft werden müssen, samt RFID-Tags und funktionierendem Netzwerk. Deswegen wird die nötige Hardware und das dazugehörige Netzwerk simuliert. In diesem Fall erfolgt die Umsetzung des RFID-Netzwerk mit Hilfe der RFID Anywhere Lösung, da es dafür alle nötigen Bestandteile bietet.

RFID Anywhere ist wie in Abbildung 2.7 gezeigt in verschiedene Komponenten mit unterschiedlichen Funktionen gegliedert. Die Abbildung stellt einen Überblick über die wichtigsten Bestandteile des iAnywhere Frameworks dar.

Simulations Daten Mit dem *Simulator Data Editor* werden die RFID Simulator Files erstellt. Um eine RFID-Umgebung zu testen, muss der Betrieb getestet oder simuliert werden. Die Simulation stellt Ereignisse, wie das Erkennen und das Auslesen von RFID-Tags dar, wie es passieren würde wenn der Tag in den Lesebereich eines RFID-Scanners gelangt. In dem Editor wird festgelegt, von welchem Typ die RFID-Tags sind. Festgelegt wird zusätzlich wann sie auftreten, wie lange sie sichtbar sind, und welche Identifikati-

[3] www.sybase.com

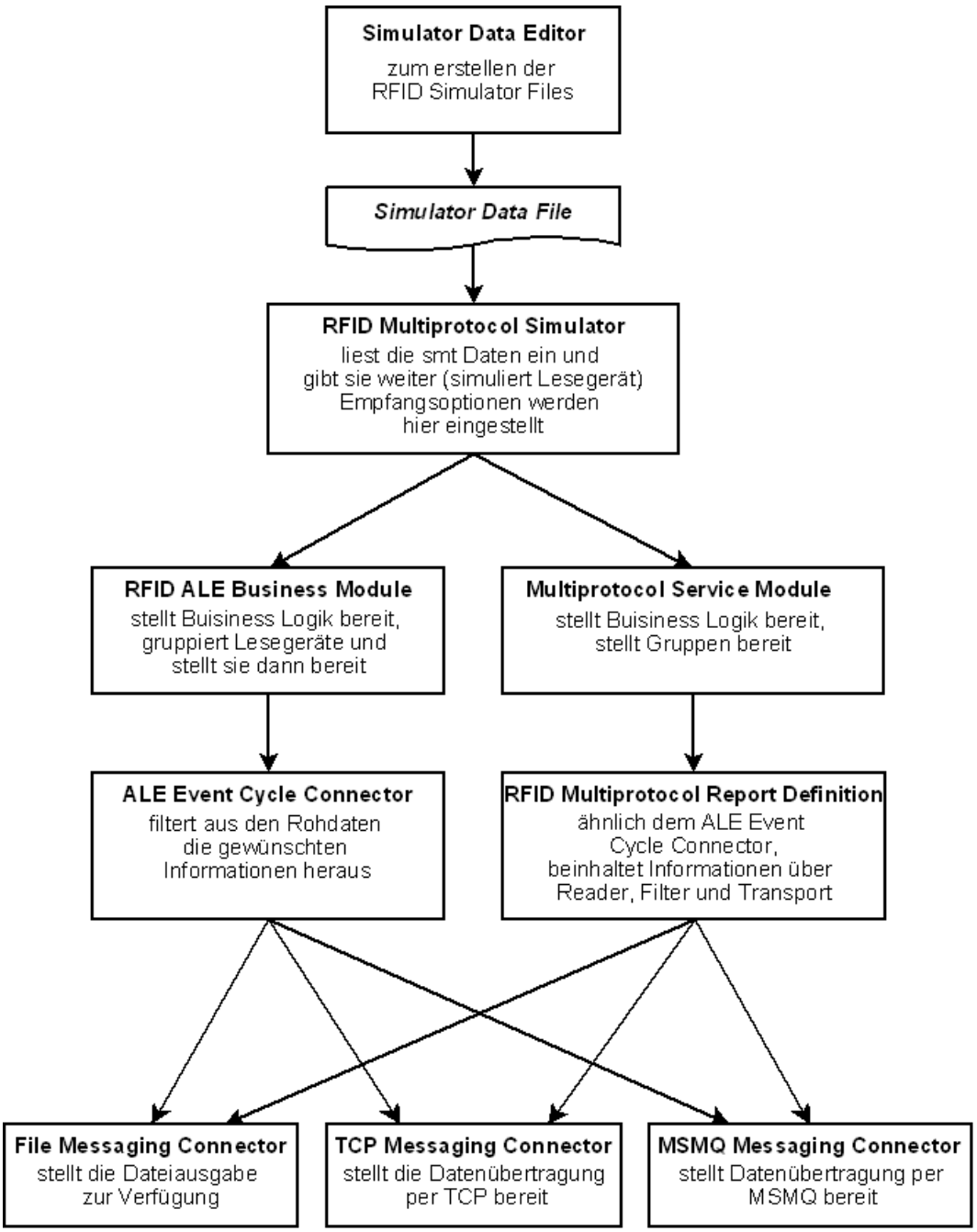


Abbildung 2.7.: Abbildung der Struktur der RFID Anywhere Architektur

onsnummer auf ihnen gespeichert ist. Damit lässt sich der zeitlicher Ablauf erkannter RFID-Tags frei simulieren, auf einer beliebigen Anzahl Lesegeräte. Unabhängig von den Simulationsdaten, werden noch einige durch das RFID Anywhere bereitgestellten Komponenten benötigt, die eine Verarbeitung und Anzeige der RFID-Daten ermöglichen.

RFID Multiprotocol Simulator Connector Der RFID Multiprotocol Simulator liest die RFID Simulator Files ein und stellt sie der Simulationsumgebung zur Verfügung. Er ist die eigentliche Simulation des Lesegerätes.

ALE Business Module ALE oder *Application Level Events* wird ein Standard der EPCglobal genannt. Er legt fest, wie die Rohdaten weiterverarbeitet und umgewandelt werden. Das ALE Business Module ist dafür zuständig, Gruppen von Lesegeräten zusammenzufassen. So lässt sich die Verarbeitung der Rohdaten auf das ALE Business Module als Quelle beschränken und das System bleibt mehr oder weniger flexibel erweiterbar. Dadurch das Lesegeräte nicht selbst angesprochen werden, sondern lediglich die Gruppe in denen sie zusammengefasst sind, lässt sich die Anzahl und der Typ der Lesegeräte hinter dem ALE Modul beliebig ändern. Die Verwaltung der Lesegeräte hängt nur von dem ALE Business Modul ab, das eine sichere unveränderliche Quelle für die dahinter liegende Logik bietet. Richtig geplant, bleibt die Simulation so ohne große Umbauten frei skalierbar und erweiterbar.

ALE Event Cycle Connector Der ALE Event Cycle Connector legt fest, welche Informationen aus den Rohdaten ausgelesen werden sollen. Bestimmbar ist, nach welchen RFID-Tags gefiltert wird, welche in der Tag-ID festgelegten Informationen ausgelesen werden sollen und in welchem Zeitrahmen dies geschehen soll. Dadurch lassen sich gefilterte Daten generieren, die nur die gewünschten Informationen enthalten und an einen der 3 beschriebenen Messaging Connector übergeben werden.

Messaging Connector RFID Anywhere bringt 3 verschiedene „Messaging Connector“ mit. Die „File Messaging Connector“ genannte Dateiausgabe als Textdatei, den TCP Messaging Connector, der seine Informationen per TCP Stream in einem Netzwerk bereitstellt und den MSMQ Messaging Connector, der eine Übertragung per Microsoft Message Queuing Kommunikationsprotokoll ermöglicht.

Multiprotocol Service Module Das Multiprotocol Service Module fasst wie das ALE Business Module ebenfalls Gruppen von Lesegeräten zusammen und stellt sie dem RFID MultiProtocol Report Definition Element zur Verfügung. *Der Unterschied zum ALE Buisiness Modul*

RFID Multiprotocol Report Definition Der RFID Multiprotocol Report Definition Konnektor erstellt, prüft und verschickt Reports im XML Format. Im Gegensatz zu dem ALE Event Cycle Connector ist das Report Engine MP schneller und leichter zu handhaben. Je nach Einstellungen liefert es die gewünschten Informationen und leitet diese zur Weiterverarbeitung z.B. an eine Enterprise Software. Im Gegensatz zum ALE Business Modul, kann die Report Engine MP auch Informationen von nicht EPC konformen Tags verarbeiten.

2.5.1. RFID Anywhere Business Module

Mit Hilfe der oben genannten Komponenten wurden die erste Test zur Simulation realisiert. Dies funktionierte in dem angegebenen Rahmen ohne Probleme. Die letzte Möglichkeit Daten innerhalb des Frameworks zu verarbeiten, ist die des RFID Anywhere Business Moduls. Business Module sind abgeschlossene Softwareeinheiten, die als Service innerhalb der RFID Anywhere Umgebung laufen. Sie sind in der .NET Umgebung von Microsoft[4] geschrieben. Technisch sind damit alle durch die Entwicklungsumgebung zur Verfügung stehende Funktionen nutzbar. Das Ziel welches mit Hilfe der Business Module

[4] http://www.microsoft.com/austria/technet/articles/600705.mspx

erreicht werden soll, ist es die generierten Daten selbst zu verarbeiten und sie nicht nur zu filtern. Dadurch lassen sich alle im RFID-Netzwerk auftretenden Ereignisse auf beliebige Art und Weise aufnehmen, verarbeiten und weiterleiten.

3. Überblick und Bewertung vorhandener Trackingsysteme

In diesem Kapitel soll geprüft werden, welche funktionierenden Möglichkeiten im Bereich des RFID basiertes Trackings existieren. Bekannt ist, dass es durchaus umfangreiche Erfahrungen in den nicht medizinischen Bereichen gibt, wie Lagerverwaltung oder Logistik. Abgesehen von den klassischen Einsatzgebieten in der Wirtschaft, soll überprüft werden, in wie weit die Technologien zur Planung, Durchführung und Kontrolle in den Bereich des Gesundheitswesens vorgedrungen sind. Dabei soll das Augenmerk auf funktionierenden Systeme für das Gesundheitswesen liegen, die ihre Aufgaben bereits erfüllen oder in naher Zukunft könnten? Zusätzlich werden auch Trackingsysteme angeführt, die nicht direkt dafür ausgelegt sind Personen zu lokalisieren. Da ihre Technik allerdings vergleichbar ist, werden sie hier mit aufgeführt.

Zu Beginn dieses Abschnitts wird ein Beispiel für den wirtschaftlichen und zeitlichen Nutzen eines RFID-Trackingsystem angeführt. Diesem folgen Projekte zur Medikamenten- und Patientenverfolgung im Uniklinikum Jena, ein System zur Patientenlokalisierung in Nizza, die komplette Überwachung des Taipei Medical University Hospitals per RFID und ein Barcode/RFID Hybrid System in Harvard. Den Abschluss bildet eine Zusammenfassung mit einem kurzen Resümee.

3.1. Beispiele für verschiedene Lösungen

3.1.1. Beispielrechnung für ein typisches Krankenhaus durch Cisco Systems

Ein Beispiel für die Lokalisierung im Krankenhaus mittels aktiver RFID-Tags sowie von WLAN Lokalisierung stellt Cisco Systems[1] vor. In diesem Beispiel steht erst einmal der wirtschaftliche Aspekt im Vordergrund. Der Kern der Untersuchung ist der Fakt, dass wichtige und häufig genutzte Geräte in einem Krankenhaus, nicht immer an ihrem eigentlich Platz zu finden. Kommen die Geräte nach ihrem Einsatz nicht zurück an ihren angestammten Platz, ist der nächste Nutzer gezwungen, diese zu suchen. Suchen kostet Zeit und der dadurch entstandene Zeitverlust Geld. Der Zeitverlust, kann die Qualität der Dienstleistungen beeinträchtigen. Dieser Aspekt steht heute aber, neben der Wirtschaftlichkeit, mehr und mehr im Fokus der Bemühungen zur Verbesserung der eigenen Abläufe.

Als Grundlage für die Berechnungen gelten folgende Rahmenbedingungen und Zahlen. Der „Asset Loss“ in Krankenhäusern, also das nicht auffinden von eigentlich vorhandenen Geräten, wird je nach Typ mit 15-20% angegeben [21]. In kleineren Krankenhäusern, mit rund 500 Betten, sind in dem Beispiel 40 von 500 Infusionspumpen bei der Wartung nicht auffindbar. Dies ergibt einen fehlenden Anteil von 8%. In Krankenhäusern mit ∼1500 Betten soll die Zahl an nicht auffindbaren Infusionspumpen bereits bei 17% liegen. Das bedeutet, dass von 1500 vorhandene Pumpen ca. 250 fehlen oder nicht aufzufinden sind.

Ließe sich mit Hilfe der RFID-Lokalisierung die Auslastung der Infusionspumpen um 20% erhöhen, wären eine geringere Anzahl vorgehaltener Infusionspumpen nötig. Da sich die geringere Anzahl besser verteilt, wäre die Einsparung bei der Gesamtzahl mit 546.000€ zu beziffern, wie aus der Tabelle 3.1 zu entnehmen ist. Die Rechnung des Autors basiert nicht nur auf den reinen Anschaffungskosten, sondern auf einer Mischkalkulation aus Investitionskosten, Miet- bzw. Leasingkosten sowie den Kosten für den Betriebs-

[1] www.cisco.com

und Wartungsaufwand. Diese Rechnung lässt sich dementsprechend auf beliebige andere medizinischen Geräte übertragen.

Anzahl Infusionspumpen im Gebrauch	Kosten pro Infusionspumpe	aktuelle Auslastung	gesteigerte Auslastung	optimierte Anzahl Infusionspumpen in Gebrauch	Kostenersparnis
500	3000€	35%	55%[2]	318	546.000€

Tabelle 3.1.: Kostenersparnis bei besserer Nutzung der vorhandenen Infusionspumpen [21]

Das verbesserte Auffinden von Geräten und Personen hat einen weiteren Vorteil. Laut [21] generiert jeder Behandlungsraum alle 15 Minuten ca. 400€ Cash-Flow. Das bedeutet, dass 15 Minuten Behandlung im Schnitt 400€ Umsatz pro Raum generieren. Wird jetzt die Behandlungszeit von 40 Behandlungsräumen über ein Jahr mit 250 Tagen zu je 9 Arbeitsstunden addiert, werden die weiteren möglichen Einsparungen durch den erworbenen Zeitgewinn ersichtlich. Die Berechnung wird unter der Voraussetzung durchgeführt, dass mehr Behandlungskapazitäten benötigt werden als verfügbar sind. In Zahlen ausgedrückt kann aus Tabelle 3.2 abgelesen werden, dass bereits eine Verbesserung um 1% bei der Ausnutzung der Arbeitszeit, ungefähr 1.400.000€ zusätzlichen Jahresumsatz bedeuten würde.

Dieses Beispiel ist nur theoretischer Natur und nicht allgemein gültig. Es gibt aber einen Hinweis darauf, wie ein gut geplantes und eingesetztes RFID-Trackingsystem Informationen liefern kann. Die dadurch gewonnene Zeit lässt sich direkt in einen finanziellen Gewinn umrechnen. Als zusätzlichen Aspekt zum betriebswirtschaftlichen Mehrwert, folgt der Zugewinn bei Dauer und Qualität der Behandlung und der damit verbunden höheren Zufriedenheit der Patienten.

[2] Die hier angegebenen 55% beziehen sich auf die Erhöhung der Auslastung. Insgesamt werden 63,64% der ursprünglich genutzten Geräte benötigt, wodurch 182 eingespart werden können.

Gesamtzeit der Behandlungs-räume pro Tag (in Minuten)	Verbesserung der Ausnutzung	Nach Optimierung benötigte Nutzungszeit der Behand-lungsräume (in Minuten)	zusätzlich verfügbare Behandlungszeit pro Tag (in Minuten)	Zusätzliches Umsatz-potential (pro Jahr)
21.600	1%	21.384	216	1.400.000€

Tabelle 3.2.: Gewinn durch Zeitoptimierung [21]

3.1.2. Aus dem Informationsforum RFID

Mehrere RFID basierte Projekte sind im Gesundheitswesen sowohl geplant, als auch umgesetzt worden. Nicht alle davon dienen lediglich dem auffinden und verfolgen von Patienten. Die denkbaren Einsatzmöglichkeiten sind vielfältig. Einige Umsetzungen, die in Kliniken Einzug halten konnten, wurden durch das Informationsforum RFID [32] vorgestellt. Die Projekte, die sich mit der Identifikation und dem Orten von Patienten befassen werden in den nachfolgenden Abschnitten erläutert werden.

Uniklinikum Jena Ein oft genanntes Einsatzfeld für die Radio Frequenz Identifikation im Gesundheitswesen ist die Medikamentenverfolgung. Dabei geht es darum, den genauen Weg und die Verwendung eines jeden Medikamentes genau nachvollziehen zu können. Im Uniklinikum Jena wurde dafür Ende 2005 ein System zur Überwachung und Dokumentation, beginnend beim Medikamententransport bis hin zur Vergabe an den Patienten, eingerichtet. Dafür erhält jeder Patient der Intensivstation bei der Anmeldung einen RFID-Transponder in Form eines Armbandes. Soll dem Patient ein Medikament verabreicht werden, liest das Pflegepersonal zuerst die Informationen des Armbandes über einen Handscanner aus. Die zu der dort gespeicherten Tag-ID gehörige elektronische Patientenakte wird daraufhin auf dem Lesegerät angezeigt. Die Verknüpfung von Tag-ID und Patientenakte ist lediglich durch das gesicherte IT-System des Krankenhauses möglich.

Die Medikamentenverpackung ist ebenfalls mit einen Transmitter bestückt, der mit dem Handscanner erfasst wird. Aus der Verknüpfung der Medikamenteninformationen und der elektronischen Patientenakte, lassen sich noch vor der Behandlung besondere Pflegeanleitungen, eventuell bekannte Unverträglichkeiten sowie Allergien anzeigen. Bei der Vergabe des Medikamentes wird der Zeitpunkt und die Dosis erfasst und in die elektronische Patientenakte eingetragen. Das Klinikum erhofft sich von diesem System vor allem eine Verbesserung bei der Patientenversorgung und Einsparungen im Bezug auf die Medikamentenlogistik. Denn ein automatisches Bestellsystem würde es ermöglichen, kleinere Medikamentenbestände vorzuhalten und den Zeitraum der Bestellverarbeitung deutlich zu verkürzen. Somit ließen sich Kosten sparen und Behandlungsschritte beschleunigen [32, Seite 6 f.].

Universitätsklinik Nizza Die Universitätsklinik Nizza zielt mit dem von IBM[3] installiertem RFID-Trackingsystems [31] einen Schritt weiter in Richtung Personentracking. Hier war es von Anfang an das Ziel, Patienten zu lokalisieren. Zur Lokalisierung dient ein RFID-Armband, das an Patienten ausgegeben wird. Zusätzlich werden ebenfalls medizinische Geräte und die Tablet PCs der Ärzte mit Transpondern ausgestattet. Eine dafür entwickelte „Complex Event Processing Engine“ hält den Kontakt zu den Tags und erfasst alle Informationen in Echtzeit. An speziellen Bildschirmen sowie über die Tablets werden sämtliche erfassten Informationen zum Patienten angezeigt. Zusätzlich können alle weiteren Daten aus der elektronischen Patientenakte abgerufen werden. Durch die Geräteüberwachung, soll sich deren Auslastung erhöhen und der Behandlungprozess insgesamt verbessern lassen [32, Seite 9].

3.1.3. Taipei Medical University Hospital

Im August 2003, begann das Taipei Medical University Hospital (∼416 Betten, 600 Mitarbeiter) nach dem Vorbild zweier Krankenhäuser in Singapur [37] ein RFID gestütztes

[3] www.ibm.com

Programm zum Auffinden, Eindämmen und Heilen von SARS [42]. SARS ist eine Infektionskrankheit, die Ende 2002 zum ersten Mal beobachtet wurde und hauptsächlich in Südostasien auftrat. Unter dem Druck einer drohenden Epidemie, wurde ein Einjahresplan zur Entwicklung eines „Location-based Medicare Service“ (LBMS) entwickelt. Die taiwanesische Regierung beteiligte sich mit 475.000 US$ an gut der Hälfte der Kosten für das RFID gestützte Echtzeitsystem, zum Auffinden und Überwachen von Personen und Objekten. Mit dem LBMS sollte es ausdrücklich möglich sein, potentielle und echte SARS Fälle zu finden und zu verfolgen. Für die Umsetzung wurden aktive Transponder mit Temperaturfühler ausgewählt. Auch wenn diese teurer als passive Tags sind, die höhere Reichweite und Genauigkeit bei der Ortung, sowie die Möglichkeit die Temperatur als Indikator für eine Infektion auslesen zu können, waren hier ausschlaggebend. Im gesamten Krankenhaus wurden insgesamt 163 Feldemitter, 41 RFID-Lesegeräte und 27 Yagi Antennen installiert. Auch die Software zum sammeln, verarbeten und speichern der Daten wurde selbst entwickelt. Das System funktionierte so gut, dass es das Krankenhausmanagement veranlasste, weitere medizinisch relevante Systeme, wie z.B. präzises Equipmenttracking, Neugeborenen Überwachung und Medikamentenüberwachung. Bei der Realisierung des Projektes wurden rückblickend folgende Probleme und Erkenntnisse festgehalten [42, S. 5 ff].

1. Die Umsetzung des RFID-Systems konnte nicht einfach eingekauft werden, denn es waren bis dato nur wenige zufriedenstellende Lösungen verfügbar. Dazu kommt, dass es weder ein reines IT-Projekt noch ein Business Projekt war. So wurde ein Gemeinschaftsprojekt geschaffen in dem sich jede Abteilung für einen anderen Bereich verantwortlich zeichnete. Jede Partei betätigte sich in seinem Spezialgebiet, koordiniert durch regelmäßige Meetings, passende Projektverantwortliche und eine Projektleitung die sich aus Verantwortlichen der einzelnen beteiligten Firmen und Abteilungen zusammensetzte. Auch das medizinische Personal des Krankenhauses, die Anwender, wurden bedacht. Sie sollten in die Entstehungs- und Entscheidungsprozesse mit einbezogen werden. Nur so ließen sich die Neuerungen in den medizinischen Alltag integrieren und die Planungen realisieren.

2. Die wichtigste Aufgabe dieses RFID-Systems ist es, ohne Lesefehler oder Verluste, Daten zu sammeln und weiterzuleiten. Nur so lassen sich Schwierigkeiten bei der Datenauswertung vermeiden. Dafür war es entscheidend genau festzulegen welche Daten erfasst, wie oft Tags ausgelesen und welche Bereiche überwacht werden sollen. Die Festlegung der benötigten Genauigkeit war dabei hauptsächlich vom gegebenen finanziellen Rahmen abhängig. Bei der Entscheidung für die aktiven Tags war der Preis wenig ausschlaggebend gewesen, da der Mehrwert an Genauigkeit und Reichweite, gegenüber den passiven Tags sehr hoch war.

3. Daten müssen nicht nur erfasst, sondern auch gespeichert werden. Gespeichert wurden diese in einer Datenbank. Bereits nach wenigen Minuten überschritt das Datenaufkommen eine Größenordnung, die nicht mehr verarbeitet und gespeichert werden konnte. Daraufhin wurde die Datenbank wieder abgeschaltet. es wurde begonnen je nach Datentyp Regeln zur Datenspeicherung festzulegen. Zum Beispiel wurde nicht mehr jeder Wert gespeichert, sondern nur noch Veränderungen des Wertes ab einer bestimmten festgelegten Größe. Die erfasste Körpertemperatur wurde deswegen nur noch bei Veränderungen um mehr als ein halbes Grad neu gespeichert. Welche Daten zwischen den einzelnen Komponenten ausgetauscht und welche überhaupt gespeichert werden sollten, wurde ebenfalls festgelegt. Ein verbessertes Datenmanagement und die Einbindung medizinischen Wissens waren hier der Kernpunkt der Verbesserung der Datenverarbeitung.

4. Der Nutzen für das Klinikum lässt sich schwer in Geld ausdrücken, denn das gesamte neu entwickelte System, beeinflusst sehr viele Bereiche im Krankenhaus. Eingeführt um SARS Infektionen zu entdecken, werden nun auch Geräte und Personen lokalisiert. Die zusätzlichen Aufgaben die zusätzlich erledigt werden, bringen einen weiteren Zeit- und Sicherheitsvorteil. Die Zeitersparnis für das Personal lässt sich konkret in Zahlen ausdrücken, die gewonnene Sicherheit generiert dagegen keinen direkten Gewinn. Ein solches System fördert neben dem effizienteren Einsatz von Ressourcen hauptsächlich die Patientensicherheit und das Vermeiden von medizinischen Fehlern, Faktoren die nicht direkt messbar sind. Ein ähnliches Beispiel für

Verbesserungen findet sich in dem Artikel „Risk Management and Measuring Productivity with POAS“ [2]. Er beschreibt den Einsatz eines POAS genannten Netzwerkes, das die Daten die in einem Krankenhaus anfallen, kontinuierlich sammelt und auswertet. Dadurch lassen sich genaue Aufstellungen und Analysen durchführen. Der Autor spricht von Kosteneinsparungen von 4 Millionen Dollar pro Jahr und einem Zugewinn von Sicherheit, der sich in verringerten Fehlerraten wiederspiegelt. Dies bezieht sich auf ein barcode-gestütztes System und die effiziente Vernetzung und Nutzung des bereits vorhandenen elektronischen Krankenhausinformationssystems. Derzeit wird das System mit RFID-Technik weiter verbessert. Bisher kamen hauptsächlich Barcodes und PDA's zum Einsatz [25].

3.1.4. Harvard hybrid system

Die Harvard Medical School gehört ebenfalls zu den Krankenhäusern mit einem RFID Pilotprojekt. Hier wurde zunächst auf ein Hybridsystem aus dem herkömmlichen kostengünstigen Strichcode System und RFID gesetzt [36]. Die aktiven RFID-Tags werden hier zum Lokalisieren von Equipment, Patientenbetten und Angestellten genutzt. Zur Wahrung des Persönlichkeitsrechts, steht es den Angestellten in Harvard aber frei die RFID-Tags nicht zu tragen. Vom Equipment wurden hauptsächlich Ventilatoren, Infusionspumpen und EKG Geräte mit Tags versehen, die laut Quelle somit jederzeit aufzufinden sind. Zusätzlich kommen passive Tags zum Einsatz, mit denen ausgewählte Patienten überwacht werden. Babys der Neugeborenen Intensivstation und Behälter mit Muttermilch wurden ebenfalls mit passiven Tags überwacht, um Verwechslungen auszuschließen. Medikamente sowie die Mitarbeiter und Patienten ohne RFID-Tag, wurde mit Hilfe der angesprochenen Strichcodes identifiziert. Die passiven Tags bewährten sich in diesem Projekt vor allem bei schlafenden Patienten und bei den Neugeborenen. Denn durch die kontaktlose Identifikation ist es möglich ohne die Patienten zu wecken oder zu bewegen sicher zu identifizieren. Die Harvard Medical School erwartet nach ersten Auswertungen des Projektes für die Zukunft, dass die Strichcodes durch RFID-Tags ersetzt werden könn-

ten, wenn die Technologie ausgereift ist und ein noch besseres Preis-Leistungsverhältnis erreicht wird.

3.2. Zusammenfassung

Die in Kapitel 3 vorgestellten Beispiele sind nicht als umfassende Aussage oder Übersicht zu RFID Trackingsystemen zu verstehen. Sie stellen einen kleinen Auswahl möglicher Lösungen dar. Es gibt weitere Beispiele, die ähnlich oder in Teilen den Beschriebenen entsprechen. Diese Beispiele zeigen, dass es RFID basierte Trackingsysteme gibt. Die Beispiele zeigen aber auch, dass sie von Grund auf neu entwickelt werden mussten. Es existiert kein universell einsetzbares oder einkaufbares System. Auch wenn ein Lieferant wie IBM das System in Nizza plant und installiert, bleibt es eine individuelle Anfertigung. Es ist sicher ein Vorteil, vor der Umsetzung die Abläufe bei der Erhebung und Verarbeitung von Daten simulieren zu können. Genauso wie die Speicherung im Vorfeld getestet werden sollte. Das Beispiel aus Taipei (siehe 3.1.3) zeigt, dass auch eine optimistische geplante Datenbank mit zu vielen unwichtigen Informationen überfordert ist. Die aktuell eingesetzten Trackingsysteme besitzen verschiedenste Aufgaben und Ziele. Die Anforderungen an diese, sind dadurch sehr unterschiedlich. Ohne die Bereitschaft ein komplettes System wie in Taipei einzuführen, werden so zunächst kleinere Projekte, wie die Verfolgung von Betten, Medikamenten oder Blutkonserven, realisiert.

Allen gemein aber ist der Wunsch nach mehr Transparenz und Effizienz im Krankenhausalltag und dem daraus resultierenden Verbesserungen im Bezug auf die Sicherheit der Patienten. Der wirtschaftliche Aspekt ist zur Zeit für viele Krankenhäuser ein überlebenswichtiger Faktor. Die Einsparungen durch erfolgreiche RFID-Systeme werden daher oft nur in wirtschaftlichen Zahlen angegeben. Eine Ausnahme stellt hier die Untersuchung aus Japan [2] dar, in der auch die verringerte Fehlerquote bei der Medikamentenvergabe wissenschaftlich festgehalten wurde. Dazu wurde in keinem der vorgestellten Projekt, von einem Nachteil für die Patienten gesprochen. Der Einsatz führte vielmehr zu einer ge-

fühlten Verbesserung der Sicherheit. Die veranlasste einige Häuser, den Funktionsumfang der RFID gestützten Systeme sukzessive weiter auszubauen [42, S. 5].

4. Machbarkeitsanalyse

Das vierte Kapitel beinhaltet eine Übersicht über die Bereiche, die bei der Einführung und Umsetzung eines RFID-Trackingsystems zu beachten sind. Dabei orientiert sich der Abschnitt zu den technische Anforderungen an den Ergebnissen der erfolgreichen Umsetzungen in Teil 3. Gefolgt von den Anforderungen an die Standardisierung in 4.2, den Datenschutz in 4.3 und die Datensicherheit in 4.4 soll dieser Abschnitt zeigen auf welcher Basis eine Umsetzung möglich wäre. Nach dem Festhalten der Mindestanforderungen für das adäquate Lösen der Aufgabenstellung, folgt als letzter Punkt in diesem Kapitel eine persönliche Einschätzung der Situation.

4.1. Die technischen Anforderungen

In den vorhergehenden Kapiteln sind verschiedene Umsetzungen für RFID-Systeme in Krankenhäusern beschrieben. In diesem Kapitel sollen nun die technischen Anforderungen an ein RFID-Trackingsystem genauer betrachtet werden.

4.1.1. Mindestanforderungen

Wie sehen die technischen Anforderungen für ein RFID basiertes Patiententrackingsystem aus? Je nachdem welcher Zweck verfolgt wird, ist der Grundaufbau unterschiedlich. Soll jedes Objekt zu jeder Zeit auffindbar sein, stellen aktive RFID-Tags die optimale Lösung das. Denn im Gegensatz zu passiven Lösungen, sind die aktiven Transponder

aufgrund ihrer Bauweise (siehe 2.1) über größere Entfernungen zu Orten. Passive Tags lassen sich weniger genau Lokalisieren, sind dafür aber deutlich billiger. Reicht die Überwachung von bestimmten Punkten oder Standorten aus, erfüllen die passiven Tags ihren Zweck. Aktive Transponder wären in diesem Fall nicht nötig, da die RFID-Tags in den Lesebereich der Lesegeräte hinein bewegt werden. Ein weiterer Punkt ist die Langlebigkeit von aktiven Transpondern. Sie sind dafür ausgelegt mehrmals verwendet zu werden. Das macht es aber nötig, sie nach der Verwendung an Menschen, zu reinigen und sie auf ihre Funktion hin zu überprüfen [14]. Werden sie dann erneut eingesetzt, muss sichergestellt sein, dass sie auf den neuen Träger registriert werden. Der RFID-Tag darf bei der Wiederverwendung nicht mehr seinem ursprünglichen Besitzer zugeordnet sein. Dies ist laut Egan et al. (siehe [14]) nicht nur eine eintönige sondern auch fehleranfällige Arbeit. Zudem wurde bei dem dort beschriebenen „Operating Room of the Future Project“ des Massachusetts General Hospital festgestellt, dass die Verwaltung und Registrierung der aktiven RFID-Tags aufwendig und zeitraubend ist. Zwar müssen auch passive Tags auch auf einen Patienten registriert werden, allerdings entfallen Aufhebung und Neuzuweisung der Registrierung. Dazu kommt der Fakt, dass sie nicht gereinigt werden müssen. Einfache passive Transponder sind zum aktuellen Zeitpunkt so billig, dass eine Reinigung teurer wäre, als sie nur einmal zu verwenden.

Mit der Entscheidung für eine bestimmte Bauform der RFID-Tags wird auch gleichzeitig die nötige Infrastruktur beschlossen, die zum Auslesen der Tags nötig ist. Lesegeräte für passive Tags werden bevorzugt an Engstellen, Türen oder aber in Bereichen, die logisch voneinander getrennt sind, aufgestellt. Die Reichweite der Tags ist mit maximal 5m gering und so müssen sie durch das ausgestrahlte lokale Feld bewegt werden. Es würde demnach reichen, alle Ein- und Ausgänge der Räumlichkeiten zu beobachten und mit Lesegeräten auszustatten. Im Gegensatz zur Überwachung der Gesamtfläche eines Krankenhauses mittels aktiver Transponder und der genauen Lokalisierung, ist dies weniger aufwendig. Bei der räumlichen Ortung aktiver Tags, müsste die komplette Fläche des zu überwachenden Bereiches abgedeckt sein. Sonst gäbe es Orte in denen die Tags nicht lesbar wären und die Integrität der Daten wäre nicht mehr gesichert. Dies würde bedeuten,

dass mehr Lesegeräte, mehr Antennen oder auch Feldgeneratoren zum Einsatz kommen müssen. Das Bedeutet gegenüber der passiven Variante, dass die Kosten für Anschaffung und Installation der Lesegeräte deutlich höher wäre. Denn die Antennen der Lesegeräte müssen ausgerichtet werden um optimale Ergebnisse zu erzielen. Das kostet zusätzlich Zeit und benötigt Erfahrung. Der Vorteil des Trackingsystems mit aktiven Transpondern, sind Daten, die ungleich genauer und vielfältiger sind. Mit ihnen ließe sich zum Beispiel der genaue Weg einer Person oder eines Gerätes verfolgen. mit ihnen lässt sich bis auf wenige Meter genau bestimmen, an welchem Ort sich der Träger gerade befindet.

Umfang und Kosten für die Infrastruktur richten sich nach der eigentlichen Größe des zu überwachenden Bereiches. Genaue Zahlen werden selten veröffentlicht, aber für das komplette mit aktiven Tags überwachte Taipei Medical University Hospital [42] waren rund 1 Million US$ geplant worden, von denen die Hälfte aus staatlichen Mitteln stammten. Ein genaue Planung der Materialkosten ist sehr vom Umfang und vom Voranschreiten der Entwicklung abhängig. Derzeit fällt der Preis für RFID-Tags weiter, da die Nachfrage nach ihnen, und damit auch die Produktionsmenge, weiter wächst [23]. Die passiven Tags kosten, wenn sie in großen Stückzahlen gekauft werden, nur noch wenige Cents, die Aktiven je nach Ausstattung dagegen noch mehrere Euro pro Stück.

Die RFID-Lesegeräte versenden ihr Daten über einen normalen Netzwerkanschluß. Je nach Ausstattung über LAN oder WLAN. Das ist ein Vorteil, da die meisten Krankenhäuser komplett mit einem physischen Netzwerk versehen sind. Das bedeutet, dass bei der Verbindung der Lesegeräte mit dem restlichen System, auf das vorhandene Netzwerk zurückgegriffen werden kann. Lediglich die Verbindung vom Lesegerät zum nächstgelegenen Netzwerkanschluss muss installiert werden. Versenden die Lesegeräte ihre Daten per WLAN, wird zwar ihr Anschluss einfacher, dafür sind die Geräte in der Anschaffung teurer. Doch die Installation der Lesegeräte stellt kein Hindernis für den Aufbau des RFID-Netzwerkes dar [6].

Die größte Schwierigkeit ist die Speicherung der Daten. Bei der Datenerhebung können je nach Ziel sehr viele Informationen erfasst werden, wie die Beispiele in Kapitel 3.2

zeigen. Die Daten zu empfangen und über das Netzwerk zu versenden ist technische ohne Probleme lösbar. Anschließend müssen die Daten gefiltert, ausgewählt, gespeichert und verarbeitet werden. Die Entscheidungen darüber, welche Daten am Schluss in einer angebundenen Datenbank gespeichert werden, muss im Vorfeld getroffen sein. Da die Informationen teilweise personenbezogene Daten enthalten, müssen sie auch mit den entsprechenden Sicherheitsmaßnahmen geschützt werden. Welche Anforderungen an den Umgang mit den Informationen gestellt werden, erläutern die Kapitel 4.3.1 und 4.4.

4.1.2. Probleme durch den Einsatz von RFID auf Medizintechnik

In einer 2008 erschienenen Studie wurde der Einfluss der Radiofrequenz-Identifikation auf medizinische Geräte untersucht. Der Test auf elektromagnetischen Interferenzen außerhalb einer klinischen Umgebung ergab, dass in 34 Fällen von 123 Versuchen Zwischenfälle[1] ermittelt wurden. 22 davon wurden als „gefährlich“, 2 als „signifikant“ und 10 als „leicht eingestuft“. Die genauen Vorkommnisse lassen sich in dem dazu erschienenen Artikel [41] verfolgen. Weiterhin wurde festgestellt, dass passive 868-MHz RFID-Tags mehr Zwischenfälle verursachten als die aktiven 125-kHz RFID-Tags. Die Zwischenfälle ereigneten sich im Schnitt bei 30 cm Abstand zwischen Lesegerät und medizinischem Gerät.

Das Fazit des Artikels ist, dass Hardware die ohne Tests aus der Logistik übernommen wurde, der Grund für die Zwischenfälle gewesen sei. Die Tests auf Interferenzen mit Medizingeräten sollten deswegen vor Ort in Krankenhäusern wiederholt und ausgeweitet werden. Dafür sollten ebenfalls internationale Standards überprüft und aktualisiert werden.

[1] http://www.amc.nl/index.cfm?pid=5266

4.1.3. Einschätzung der technischen Anforderungen

Die theoretische Planung für die Erfassung der RFID-Tags sieht vor, lediglich die Ein- und Ausgänge von Räumen zu überwachen (Siehe Abschnitt 5.1.1). Eine genaue Positionsbestimmung wird damit nicht möglich, es lässt sich aber ermitteln, in welchen Räumen sich der Patient aufgehalten hat. Für ein Szenario, in dem Personen nicht genau lokalisiert sondern nur ihr Durchlauf durch verschiedene Räume aufgezeichnet wird, ist die Nutzung von passiven RFID-Tags und den entsprechenden Lesegeräten an strategisch sinnvollen Stellen ausreichend. Für die Patientenpfade interessieren zunächst nur die Wege und die daraus resultierenden Zeiten die an bestimmten Orten verbracht werden. Das genaue Positionsbestimmung von Personen und Gegenständen mit aktiven Tags wird erst sinnvoll, wenn eine passende Nutzung der daraus bezogenen Informationen vorliegt. Denn nicht in jedem Bereich ist die komplette Überwachung sinnvoll oder nötig. Erst bei der Umsetzung weiterer Aufgaben, wie zum Beispiel der Überwachen geistig verwirrter Personen oder der Nutzung von Sensordaten von RFID-Tags, werden aktive RFID-Tags und die damit verbundenen Erweiterungen sinnvoll. Um größere Geräte und Personen zu finden ist es in den meisten Fällen ausreichend, zu wissen in welchem Raum sie sich befinden oder zu letzt befunden haben. Sollte erkennbar sein, dass eine genauere Ortung sinnvoll wäre, ist es zudem möglich später auf aktive RFID-Tags umzurüsten.

Die Probleme mit Medizingeräten die im vorherigen Abschnitt 4.1.2 genannt wurden, sind in diesem Fall nicht unerheblich. Denn die untersuchten Geräte bezogen sich meistens auf lebenswichtige Geräte der Intensivmedizin. Das ist im Fall der Untersuchung im Bereich der Patientenaufnahme ein geringeres Problem, da dort weniger medizinische Geräten zum Einsatz kommen. Dennoch bleiben weitere Untersuchungen zu diesem Thema abzuwarten. Alternativ müsste der Einfluss des passiven Trackingsystems auf vorhandenes medizinischen Gerät geprüft werden.

Neben dem Aufbau der reinen Hardware ist auch die dahinter stehende Softwareplattform von entscheidender Bedeutung. Richtige Planung und Simulation können später Ausfälle oder unnötige Nachbesserungen vermeiden. Die Installation eines Systems mit

passiven Tags, ist für die gestellte Aufgabe ausreichend und weniger kostenintensiv im Vergleich zu einem Trackingsystem mit aktiven RFID-Tags. Eine Nachrüstung und Integration in bereits genutzte Gebäude und Infrastrukturen ist durch die geringere Anzahl Lesegeräte leichter umzusetzen. Die leichtere Handhabung der passiven Einwegtransponder ist ein weiterer Vorteil dieser Variante. Durch die Beschränkung auf die Überwachung der Ein- und Ausgänge fallen weniger Daten an, was deren Menge verringert und die technischen und organisatorischen Anforderungen an die Datenbank herabsetzt.

So ist ein einfaches System mit Lesegeräten an den wichtigen Wegpunkten, die sie sich einfacher installieren lassen, für die geplante Aufgabe ausreichend. Es hat gleichzeitig den Effekt weniger Daten zu produzieren als ein System zur genauen Positionsbestimmung. Damit wäre auch die Skalierung sowie die Erprobung der Softwarekomponenten weniger aufwendig und für die Aufgabenstellung ausreichend.

4.2. Standards zur RFID-Tag Kennzeichnung

Zur Identifikation von RFID-Tags gehört eine unverwechselbare Identifikationsnummer. Das bedeutet, dass es das Ziel ist, die Tag-ID so zu gestalten, dass sie eindeutig ist und dabei noch zusätzliche Informationen enthält. Gleichzeitig muss die Tag-ID möglichst Platzsparend sein, da gerade passive RFID-Tags nur über wenig Speicherplatz verfügen. Wie sollte die Kennzeichnung der Tags deshalb gewählt werden?

Im Bereich des Gesundheitswesen gibt es bisher keinen explizit ausgewiesenen Standard für die RFID Kennungen. Es gibt mit dem EPC ein Standard, der vor allem aus dem Bereich der Produkt- und Konsumgüter stammt. Dort ist der EAN-Barcode weit verbreitet [4]. Dieser ist die Grundlage für den EPC und soll hier auf seien Eignung für den Einsatz im Gesundheitswesen vorgestellt werden. Außerdem wird der vom Health Industry Business Communication Council (HIBCC) und dem dazugehörige europäischen Verband EHIBCC eingeführte Standard für die 2D und RFID Kennzeichnung betrachtet.

4.2.1. EPC Tag

Wie bereits in Kapitel 2.3 beschrieben ist der EPC ein eindeutiger individueller Identifizierungscode für Objekte. Er setzt sich aus 4 Teilen zusammen, welcher einen weltweit eindeutigen Schlüssel zur Identifizierung bildet. In diesem Kapitel werden der genaue Aufbau des EPC's und die zugrunde liegenden Standards beschrieben. Es soll weiterhin geklärt werden, ob es für den EPC spezielle Normen für den Gesundheitssektor gibt.

Der EPC wird in den Speicher des RFID-Tags geschrieben und enthält neben dem EPC noch zusätzliche Datenfelder (siehe Abbildung 4.1).

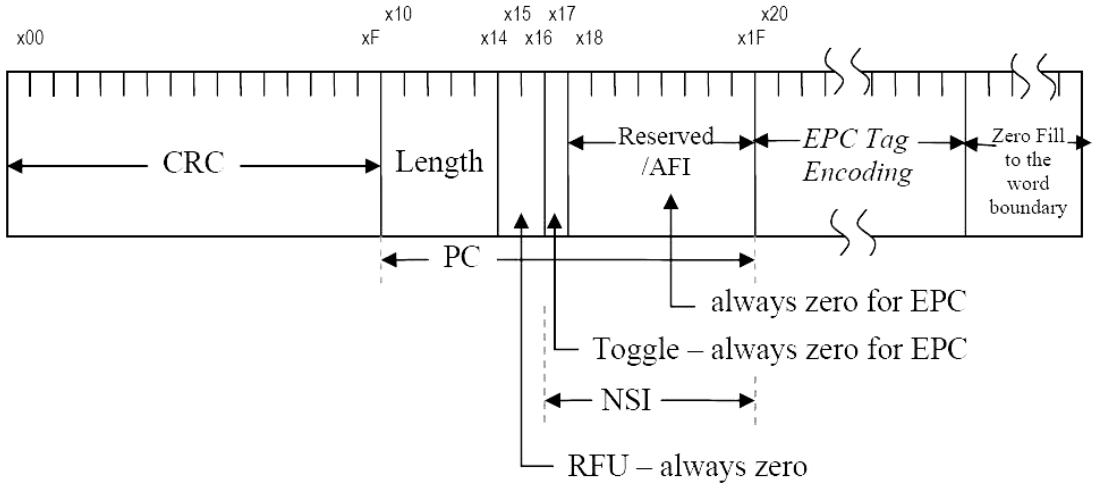


Abbildung 4.1.: schematischer Aufbau eines RFID Gen 2 Tag [17]

Der komplette EPC unterteilt sich in die in Abbildung 4.1 angegebenen Bereiche. Das gezeigte Schema bezieht sich auf die aktuelle Generation, die RFID Gen 2 Tag Codierung.

Die Bereiche enthalten folgende Informationen:

CRC dieser Bereich enthält eine Prüfsumme die automatisch bei der Erzeugung des Tag erstellt wird.

PC oder auch *Protocol-Control* Bereich enthält die Felder:

Length zeigt dem RFID-Lesegerät, wieviel Speicher auf dem RFID-Tag belegt

ist. Er ist dabei aber nur eine Näherung und wird ermittelt indem die Länge des genutzten Speichers (ohne den CRC) in 16 bit Bereiche unterteilt wird. Deren Anzahl wird anschließend hier angegeben. Die eigentliche Länge des EPC Codes wird dagegen ausschließlich durch seinen eigenen Header bestimmt.

RFU oder **R**eserved for **F**uture **U**se ist in dieser Protokoll Version immer 0

NSI der **N**umbering **S**ystem **I**dentifier ist die Oberbezeichnung für folgende Felder:

Toggle bit Anzeiger für EPC oder ISO Standard. Wenn er 1 ist, enthält der nachfolgende Bereich einen ISO *Application Family Identifier (AFI)* (siehe dazu Abschnitt 4.2.2.3), für EPC Tags ist dieses Bit 0

Reserved/AFI wenn das *Toggle bit* 1 gesetzt ist, steht hier der *AFI*, ansonsten wird er ausschließlich mit Nullen gefüllt

EPC Tag Auf den *PC* Bereich folgt der eigentliche Electronic Product Code. Die Bereiche davor dienen hauptsächlich der Unterscheidung der verschiedenen Typen der Codierung. Abhängig vom *Toggle bit* steht hier der EPC oder der Rest der ISO Kennzeichnung, der durch den *AFI* angekündigt wurde.

Zero fill enthält soviele Nullen, bis die durch das *Length* Feld angegebenen Zahl der 16 Bit Bereiche gefüllt sind.

Der EPC lässt sich in 7 verschiedene Typen einteilen. Unterschieden wird nach der Serialized Global Trade Item Number (SGTIN), dem General Identifier (GID), dem Serial Shipping Container Code (SSCC), der Serialized Global Location Number (SGLN), dem Global Returnable Asset Identifier (GRAI), dem Global Individual Asset Identifier (GIAI) und der Datenstruktur, die durch das amerikanische Department of Defense verwendet wird (DoD). Der Grundaufbau ist jeweils sehr ähnlich. Er unterscheidet sich oft nur hinsichtlich der Länge der einzelnen Abschnitte, ihrer Bezeichnung oder deren genauem Zweck. Eine sehr genaue Übersicht dazu findet sich in den EPCglobal Tag Data

Standards [17, Seite 25 ff].

4.2.1.1. Kodierung des EPC

Ganz allgemein besitzt jeder EPC einen 8-bit langen Header, dem eine Serie von Ziffern folgt. Der Bereich hinter dem Header ist wie bereits in Abschnitt 2.3 erwähnt in mehrere Felder unterteilt, deren Zusammensetzung durch den Header definiert wird. Falls in Zukunft einmal längere Header nötig werden, ist 11111111 die Anzeige dafür, dass ein erweiterter Header folgt. Damit ergeben sich 255 verschiedene zur Zeit mögliche Header, von denen viele noch nicht vergeben sind. Eine Übersicht über die möglichen Header sehen sie in Tabelle B.1. Auf den Header folgen in den meisten Fällen noch zwei Felder mit jeweils 3 Bit, die zur Filterung und zur Aufteilung des EPC Codes dienen. Die daran anschließenden Felder sind von der Bedeutung her immer gleich. Zuerst folgen 20-40 Bit für die Kennung des EPC Besitzers, dann der Code für den Objekttyp. Die Länge des Feldes für den Objekttyp ist je nach Typ unterschiedlich lang. Als letztes kommt die individuelle Seriennummer, die das Objekt genau beschreibt. Je nach Typ des EPC's ist auch dieses Feld verschieden lang.

4.2.1.2. EPC Beispiel

Beispielhaft soll hier ein SGTIN-96 EPC Tag kodiert bzw. dekodiert werden. Der Aufbau ist schematisch im Tabelle 4.1 aufgeführt. Wie jeder EPC Tag beginnt er immer mit dem 8 Bit langem Header. Gleich darauf folgt der 3 Bit lange Filter, bei dem die 001 für eine Einzelhandelsware, die 010 für eine Standard-Handelswarengruppe und die 011 für eine einzelne Schiffs- oder Verbrauchsguteinheit steht. Die 000 steht für alle anderen Typen, während die fehlenden vier Codes noch reserviert sind. Dazu kommen noch weitere 3 Bit mit der Angabe an welcher Stelle die Company ID und der Objekttyp getrennt werden. Dies ist notwendig, da wie bereits bekannt, beide Nummern unterschiedlich lang sein können. Die Übersicht über die Möglichkeiten der Trennung erhalten sie im Anhang in Tabelle B.2. Die nächsten 44 Bit teilen sich, je nach Partition Code, der Company Prefix

und die Item Reference. In der Summe beschreiben sie dann eine Länge von 44 Bits. Am Ende und 38 Bit lang, folgt die Seriennummer des Tags, die ihn einmalig macht. Durch seine Länge lassen sich über 274 Milliarden Artikel einer Gruppe kodieren (siehe Tabelle 4.1).

	Header	**Filter Value**	**Partition**	**Company Prefix**	**Item Reference**	**Serial Number**
SGTIN-96	8	3	3	20 – 40	24 – 4	38
	0011 0000 (Binary Value)			999,999–999,999,999,999 (Max. decimal range)	9,999,999–9 (Max. decimal range)	274,877,906,943 (Max. decimal value)

Tabelle 4.1.: EPC SGTIN-96 Bit Verteilung [17]

Damit würde sich z.B. folgender in Tabelle 4.2 aufgeschlüsselter EPC Tag kodieren lassen. Der Übersichtlichkeit halber ist zu beachten, dass der Tag in seine einzelnen Teile zerlegt wurde. Normalerweise werden die 96 Bit einfach hintereinander weg geschrieben. Die Angabe der Dezimalwerte dient zur Veranschaulichung der Binärwerte.

Feld	**Binär**	**Dezimal**
Header	00110000	48
Filter	000	0
Partition	100	4
Company ID	000010000010010001011111101	04268797
Objekttyp	00101101111111010	23546
Seriennummer	000000000000000000001111000100100000	0000000123456

Tabelle 4.2.: Beispiel für SGTIN-96 Kodierung

Der so entstandene Code kann noch in einer weiteren Form angegeben werden. Die GS1,

die Organisation welche die Standardisierung des Barcodes und des EPCs betreut, nutzt dazu den Uniform Resource Identifier (URI). Die GS1 gibt seine EPCs in einer Unterart der URI, dem Uniform Resource Name (URN) Schema an. Der Anzeiger dafür ist die Kennzeichnung „urn“. Insgesamt sieht der schematische Aufbau für einen umgewandelten EPC dann wie folgt aus:

urn:epc:tag:sgtin-96:*Filter.GeneralManagerNumber.ObjectClass.SerialNumber*

Da der Header nicht benötigt wird, sind nur die letzten Drei Felder des EPC's für den URI umgewandelt. Die Angaben die sonst im Header stehen sind in der Präambel festgehalten. So ist der URN Namespace als „epc“ festgelegt und mit „sgtin“ der Typ des EPC's definiert. Der Rest, sind die Dezimalwerte der vorher im Binärcode festgehaltenen Daten. Das obiges Beispiel aus der Tabelle 4.2 sähe als URI wie folgt aus:

urn:epc:tag:sgtin:0.04268797.23546.123456

Der Vorteil der URI ist, dass die Länge der Seriennummer des EPCs ohne Bedeutung ist. Bei längeren EPCs wie SGTIN-198 musste der komplette ungenutzte Platz mit Nullen aufgefüllt werden um immer auf die angegebene Anzahl Ziffern zu gelangen. In dieser Angabe werden die führenden Nullen des Feldes weggelassen und eine äquivalente Dezimalzahl einfach an seine Position geschrieben. Dadurch bleibt der EPC eindeutig und die Darstellung vereinfacht sich. Für die anderen möglichen Kodierungstypen des EPCs, wird die selbe URI-Form, mit angepassten Inhalten verwendet.

4.2.1.3. EPC Global Standards für den Gesundheitsbereich

Es gibt im Moment einige Projekte zum Thema Gesundheitswesen und EPC aber es sind noch keine eindeutigen Ergebnisse zur Produktkennzeichnung im Gesundheitsbereich verfügbar. Am ehesten werden wohl Arzneimittel und Medizinprodukte mit einem GTIN Ableger versehen werden, aber genaueres dazu ist noch nicht bekannt. Es gibt Projektgruppen der EPCglobal™ die an einer Umsetzung arbeiten wie die HUG™ [2] oder

[2] http://www.gs1-germany.de/internet/content/projekte/gesundheitswesen

die GS1 Healthcare[3].

4.2.2. eHIBC Tag

Dieser Abschnitt erläutert den vom EHIBCC vorbereiteten Standard eHIBC. Das zweite genannte Schema zur Kodierung von RFID Kennungen, beschreibt einen einheitlichen RFID ISO/IEC Identifikationscode. Die Grundlagen dafür basieren auf den amerikanischen Richtlinien der HIBCC zu Barcodes und 2D Datenmatrizen [15]. Die Fortführung und Umwandlung von bestehenden funktionierenden Produktkennzeichnungssysteme hat den Vorteil, dass die bisherigen ISO Kennzeichnungssysteme der Nutzer nicht geändert werden müssen. So kann jeder bisherige und zukünftige Inhaber eines „Labeler Identification Codes“ (LIC) oder „Company Identification Codes“ (CIN), die durch die HIBCC nach ISO/EIC 15459 vergeben werden, diese Kennzeichnungen direkt in seine RFID-Tag Kennung übertragen. Damit hält sich der Aufwand der Umstellung in Grenzen und gewährt die volle Kompatibilität zwischen Barcodes und RFID Kennung. Im Gegensatz zum EPC Ansatz werden die zum RFID-Tag gehörenden Informationen aber auch nicht zentral durch die verantwortliche Organisation gespeichert, sondern dezentral von jedem Hersteller oder Nutzer selbst. Damit ist man in der Lage die bisherigen Richtlinien zur Kennzeichnung zu übernehmen und an die RFID Bedürfnisse anzupassen. Allerdings beschreibt dies nur die Tag ID selbst, nicht deren Übertragung, das Datenmanagement oder ähnliches. Wie in Tabelle 4.3 zu sehen ist, wurde dies bereits in anderen ISO/IEC Dokumenten durch die EHIBCC festgehalten [26].

imFebruar 2005 brachte auch die GS1 ihren EPC in den offenen ISO/IEC 18000-Part 6 RFID Standard ein. Durch die Offenlegung der EPC Nummern und Kennzeichnung ist somit eine echte Interoperabilität zwischen den verschiedenen Systemen möglich [16].

[3] http://www.gs1.org/sectors/healthcare/

RFID Technology			
Air Interface	RFID-Tag	ISO/IEC 18000-x	2,3,4 or 6
RFID Tag memory	Memory management	ISO/IEC 15962	
RFID Data protocol	Data protocol	ISO/IEC 15961	
Unique RFID-Tag-ID	UID	ISO/IEC 15963	
Data Layer for transmissions			
Rules for Unique Item ID's	Uniqueness	ISO/IEC 15459	
Data Identifiers	DI's	ISO/IEC 15418	ASC MH10
Data Elements	Data	Application	

Tabelle 4.3.: Übersicht zu RFID bezogenen ISO-Standards [15]

4.2.2.1. eHIBC Klassen

Der eHIBC ist in drei Klassen eingeteilt. In den Unique Item RFID-Tag (**eHIBC-I**), den Product RFID-Tag (**eHIBC-P**)und den Transport RFID-Tag (**eHIBC-T**).

eHIBC-I Der *Serialized Item* Typ ist konzipiert für Dinge, die eine weltweit eindeutige einmalige Seriennummer benötigen, besonders für Gegenstände gleichen Typs.

eHIBC-P Der *Unique Product ID* Typ wird für Dinge verwendet, deren Verlauf verfolgt wird. Auf ihnen werden die einmalige Produkt ID und je nach Wunsch weitere sekundäre Daten, wie zum Beispiel Zufallszahlen oder Mindesthaltbarkeitsdaten, gespeichert.

eHIBC-T Der *Serialized code for logistical/transport units* wird für logistische Paketeinheiten wie Paletten, Kisten, etc. verwendet. Der Code dafür wird normalerweise noch mit einer Advance Shipping Notice (ASN) verknüpft, die weitere Informationen wie Inhalt und Bestellmodalitäten zur Lieferung beinhaltet.

Zur *Unique Produkt ID* oder auch *einmaligen Produkt ID* ist zu sagen, dass jeder Hersteller von RFID-Tags seine Tags mit einer einmaligen Nummer versieht. Dadurch wird jeder RFID-Tag unverwechselbar. Diese wird auch verwendet, wenn keine weiteren Anwendungsdaten verwendet oder auf dem Tag gespeichert werden.

4.2.2.2. Kodierung des eHIBC

Der eHIBC Tag ist in vier Bereiche unterteilt, wie in Abbildung 4.2 zu sehen ist. Diese vier Bereiche werden später zusammengesetzt in den Datenbereich des RFID-Tags geschrieben. Für den vollständigen Tag ist noch ein Präfix nötig.

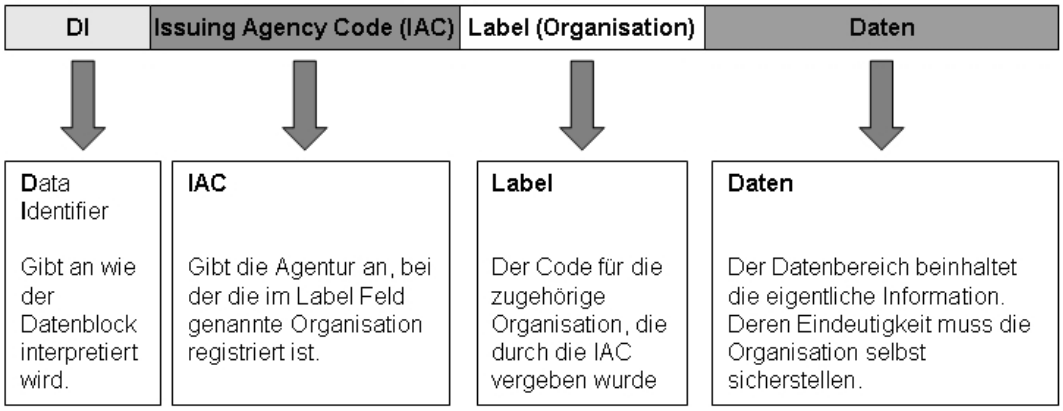


Abbildung 4.2.: allgemeine Struktur des eHIBC Codes [26]

Der *Data Identifier* (DI) kann ganz unterschiedliche Daten angeben, siehe Tabelle 4.4. Sowohl die schon bekannten vier eHIBC Typen, also auch ganz unterschiedliche weitere zusätzliche Daten. So wurde zum Beispiel festgelegt, das „14D“ ein Ablaufdatum codiert, oder „2L“ für die Kodierung der Postleitzahl von Lieferadressen steht. Für weitere DI's siehe [26].

Der *Issuing Agency Code* (IAC) gibt an, von welcher Zulassungsstelle die Organisation ihre Kodierung bekommen hat. „LH“ steht hier zum Beispiel für die HIBCC oder „LD“ für das amerikanische Verteidigungsministerium.

Gleichzeitig ist der IAC auch der Anzeiger für den folgenden *Label Code* (LIC). Dieser enthält die kodierte Kennzeichnung der zugelassenen Organisation.

Das letzte Feld enthält dann die eigentlichen Daten. Dies muss aber nicht nur eine Seriennummer sein. Je nach eHIBC ist dies auch ein Produktcode, eine zufällige Nummer oder eine beliebige andere Information. Der DI gibt an welche Art von Daten hier enthalten sind.

DI	**Beschreibung**	**Aufbau nach ISO/IEC 15459**
25P	Weltweit einmaliger Produktcode	*DI* - *IAC* - *LIC* - Produktcode
25S	Weltweit einmalige Seriennummer	*DI* - *IAC* - *LIC* - Seriennummer
25T	Weltweit einmalige Zufallsnummer	*DI* - *IAC* - *LIC* - Zufallsnummer
nJ	Weltweit einmalige Transportnummer	*DI* - *IAC* - *LIC* - Transport ID (fortl.)
18V	Weltweit einmaliger Liefercode	*DI* - *IAC* - *LIC* - Organisationseinheit

Tabelle 4.4.: Übliche DI's unter ISO/IEC 15459 [26]

4.2.2.3. Speicherformat auf RFID-Tags

Soll der Code auf den RFID-Tag gespeichert werden, so wird der DI in seine *Object ID* (OID) umgewandelt. Denn um RFID-Tags massenweise zu erfassen müssen sie eindeutig identifizierbar sein. Dies wird erreicht, indem ein *Application Family Identifier* (AFI) Code und ein *Application Sub Family* (ASF) *Identifier* Code vorangestellt wird. Die genaue Umwandlung des insgesamt 8 Byte langen Präfix ist in den ISO/IEC 15961 und 15962 Dokumenten festgehalten. Als Beispiel siehe [26, Seite 18/19].

4.2.2.4. Beispiele für den eHIBC

Stellvertretend für die verschiedenen Standards, werden hier zwei Beispiele genannt. Zum einen, der normaler eHIBC-I Code und ein Beispiel für einen aus mehreren Datenbereichen zusammengesetzten Code.

Die Struktur eines eHIBC-I Tags ist aus Tabelle 4.4 bekannt und sieht dann in seine Einzelteile zerlegt und in Tabellenform präsentiert, wie in Tabelle 4.5 aus:

	DI	**IAC**	**LIC**	**Seriennr. (1-13 Stellen)**
Weltweit einmalige Seriennummer	25S	LH	H123	123456789

Tabelle 4.5.: Aufbau eines eHIBC-I Tags [26]

Zusammengesetzt entsteht daraus der entsprechende Schlüssel:

25SLHH123123456789

Der selbe Code würde auch im dazugehörigen Barcode oder 2D Code verwendet werden.

	DI	IAC	LIC	Produktcode (1-13 Stellen)	Maß-einheit DI	Maß-einheit	Serien-nummer DI	Serien-nummer
Weltweit einmaliger Produktcode	25P	LH	H123	123456789	26Q	0	S	123456789

Tabelle 4.6.: Aufbau eines zusammengesetzten Tags [26]

Zusammengesetzte Codes sind der bisher bekannten Struktur sehr ähnlich. Die zusätzliche Information wird einfach an das Ende des ursprünglichen Tags angefügt. Die in Tabelle 4.6 gezeigte Struktur, ist die eines eHIBC-P Tags, an den zusätzliche Informationen angehängt wurden. Die Verkettung von Informationen erfolgt beim 2D und Barcode über ein „ + “. So sähe der Datenbereich des resultierende eHIBC-P Tags in der für den 2D oder Barcode angedachten Form zusammengesetzt wie folgt aus:

25PLHH123C123456789+26Q0+S123456789

Wird der Code auf einem RFID-Tag gespeichert, so wird dieser nach den in den ISO/IEC 15961 und 15962 festgelegten Regeln umgewandelt und erweitert. Aus der zwei-

dimensionalen Variante:

25PLHH123P123456+26Q1+14D20060930+1TL123456

geht der für RFID codierte Tagschlüssel hervor:

11:1:0:10:25P:LHH123P123456+26Q1+14D20060930+1TL123456

11:1:0:10 ist dabei der Präfix für den RFID-Tag, wobei dieser wie folgt zerlegt wird:

- 11 = Applpication Family ID
- 1 = ApplicationSub Family
- 0 = Access Method
- 10 = Data Format

⇒ In diesem Fall ist aber zu beachten, dass die Zeichen „+“ und „:“ des gesamten RFID-Tag Codes hier nur zur Veranschaulichung dienen. Der eigentliche RFID-Tag Code wird im Gegensatz zu den 2D Daten ohne diese Zeichen geschrieben und ist die um „+“ und „:“ reduzierte Folge von Zeichen:

11101025PLHH123P12345626Q114D200609301TL123456

4.2.3. Kompatibilität zwischen EPC und eHIBC

Der eHIBC ist je nach Einsatzzweck voll kompatibel zum EPC. Das eHIBC System ist darauf ausgelegt ASCII Zeichen zu verwenden. Der EPC ist ein numerisches System und damit vom Zeichensatz her kompatibel. Da beide Systeme die einmalige Unique RFID-Tag-ID(UID) verwenden sind sie kompatibel zueinander und stimmen inhaltlich wie in Tabelle 4.7 beschrieben überein.

[4] Die Angabe der Länge hängt immer von der Länge der ID des Unternehmens ab. Ist die LIC länger, so ergibt sich eine Seriennummer mit weniger Stellen. Dies gilt auch für die weiteren Werte der Tabelle, in denen die Maximalwerte kleiner sind als die ersten Angaben eines Bereiches. [17, Seite 24 ff]

RFID type	UID & flags nach ISO/IEC 15961, 15962, 15963	DI / Header	ID des Unternehmens (Anzahl Stellen)	einmalige Produktnummer (Anzahl Stellen)	einmalige Seriennummer (Anzahl Stellen)	einmalige Transportnummer (Anzahl Stellen)
eHIBC-I	x	25S LH	4		1-13	
eHIBC-P	x	25P LH	4	1-13		
eHIBC-T	x	J LH	4			1-20
EPC GIAI	x	14	20-40		63-42[4]	
EPC SGTIN	x	14	20-40	24-4	38	
EPC SSCC	x	14	20-40			32-17

Tabelle 4.7.: Übersicht zur Kompatibilität des eHIBC zum EPC [26]

4.2.4. Einschätzung der Standardisierung

Für die Wahl des RFID-Tag Standards reicht eine Suche nach einem Marktführer alleine nicht. Derzeit überwiegen weder der eHIBC noch der EPC im Gesundheitssektor eindeutig. Beide hier vorgestellten Möglichkeiten verbinden traditionelle Kennzeichnungssysteme mit der RFID-Tag Kodierung. Der EPC hat dabei einen etwas anderen Ansatz. In einem von der EPCglobal verwalteten weltweitem Netzwerk, werden die Produkt und Tag-Informationen gespeichert und abgerufen. So lassen sich Produktdaten mit der gespeicherten Tag-ID verknüpfen ohne das die Daten auf dem Tag selbst gespeichert sind. Die Umsetzung des Netzwerkes steht aber noch aus. Weiterhin ist fraglich, ob es für eine Anwendung wie sie hier beschreiben wurde, notwendig ist von überall her Daten abrufen zu können. Lizenzgebühren zur Nutzung des weltweiten Service wären ein weiterer einzuplanender Faktor. Diesen Service zu nutzen ist erst sinnvoll, wenn es zum Beispiel zu einer Standardisierung der elektronischen Patientendaten käme und diese zum Austausch mit anderen Netzwerkteilnehmern zur Verfügung gestellt werden sollten.

Der eHIBC Standard, der explizit auf den Gesundheitssektor ausgelegt ist, stellt in

unserem Fall die bessere Standardisierung dar. Eingeführt zum Identifizieren und Kennzeichnen von Medizinprodukten wäre sein Einsatz auch für Patienten denkbar. Dieser könnte abstrakt wie ein medizinischer Posten innerhalb des Krankenhauses definiert werden. Die Art und Weise der Kodierung entspricht den heutigen gängigen Anforderungen und lässt durch seine ASCII Kodierung auch für die Zukunft genug Möglichkeiten der Speicherung zu. Weiterhin ist es hier leicht zusätzliche Informationen auf den Tags zu speichern. So sind zukünftige Ansätze für eine weitergehende Nutzung der RFID-Tags innerhalb des Krankenhauses ebenfalls gegeben. Der eHIBC ist ein offener Standard, der die bisherigen ISO Kennzeichnungssysteme in 2D und als Barcodes unterstützt, beziehungsweise nutzt. Insgesamt stellt der eHIBC Standard im Vergleich mit dem EPC die bessere Lösung zur Verfügung. Er ist kostengünstiger, beruht auf offenen Standards und ist spezielle für den Medizinsektor aufgestellt worden.

4.3. Datenschutz

Die bisherige Betrachtung der RFID Analyse erfolgte unter technischen Gesichtspunkten. Doch bei allen technischen Details und Vorteilen der RFID-Technik, muss im Zusammenhang mit RFID auch die Frage nach dem Recht auf Datenschutz für die Nutzer gestellt werden. RFID macht viele Beobachtungen und Datenerfassungssysteme erst möglich. Im Gegensatz zu anderen Kennzeichnungs- und Erkennungssystemen arbeitet die Radio Frequenz Identifikation kontaktlos. Einerseits macht es diese Beobachtungen erst möglich, andererseits ist es gerade die nicht störende und die damit nicht zu bemerkende Identifikation, die das größte Risiko darstellt.

RFID stellt eine ernst zunehmende Bedrohung für das Recht auf informationelle Selbstbestimmung dar. Bei allen Vorteilen die dadurch entstehen, birgt es das Risiko des ungewollten und unbemerkten Auslesens der Informationen der RFID-Tags. Dadurch lassen sich die Informationen der möglichen verschiedenen RFID-Kennungen sowohl miteinander als auch mit den personengebundenen Daten des Nutzers in Verbindung bringen.

Geschieht dies ohne die Kenntnis oder das Einverständnis des Betroffenen, liegt ein Missbrauch vor [12]. In diesem Kapitel sollen bereits bestehende Vorschriften, Gesetze und Notwendigkeiten im Umgang mit personenbezogenen Daten angeführt und eine Empfehlung für den richtigen Umgang beim RFID basierten Tracking von Personen gegeben werden.

4.3.1. Vorschriften und Gesetze

4.3.1.1. Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung wurde 1982 durch das „Volkszählungsurteil“ aus dem Grundrecht für freie Entfaltung der Persönlichkeit und der Achtung der Menschenwürde abgeleitet. Es besagt, dass der Einzelne grundsätzlich selbst entscheiden darf, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden[5]. Weiterhin wurde festgehalten, dass es für jede Person auch unter veränderten technologischen Bedingungen grundsätzlich m sein muss, über die Erhebung, Verarbeitung und Nutzung seiner Daten zu bestimmen. Mit dem Recht auf informationelle Selbstbestimmung, wurde eine Grundlage geschaffen, die auch unter Berücksichtigung neuer Technologien gelten muss. Damit sollen Verletzungen der Privatsphäre verhindert werden, die bei der Schaffung des Grundgesetzes so nicht abzusehen waren [27]. Das Ergebnis dieser Bestrebungen ist im Bundesdatenschutzgesetz festgehalten.

4.3.1.2. Bundesdatenschutzgesetz

In nächsten Abschnitt soll es nicht um die Einhaltung der allgemein gültigen Datenschutzgesetze gehen, sondern Bezug nehmen zum Umgang mit personenbezogenen Daten. Die Rahmenbedingungen dafür sind in Deutschland und Europa, durch die Ausrichtung an den verschiedenen europäischen Datenschutzrichtlinien, gegeben. Im internationalen Vergleich zählen sie zu den umfangreichsten Gesetzesvorlagen. Trotzdem hielt das Bun-

[5] BVerfGE 65, S. 1.

desverfassungsgericht bereits mehrfach fest, dass „wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch Rechtsetzung korrigierend einzugreifen ist.“ [6]

Durch den Einsatz von RFID beim Tracking von Personen, gerät die Anwendung dieser Technologie in den Bereich der Personenbezogenen Daten, und damit in den Wirkungsbereich des Bundesdatenschutzgesetzes (BDSG) [8]. Dessen Zweck ist es, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“ [7]. In dem BDSG ist ebenfalls festgehalten, wie der Umgang mit personenbezogene Daten in die Erhebung, die Verarbeitung und das Nutzen eingeteilt ist. Das Erheben von Daten, bezeichnet das Beschaffen der Daten über den Betroffenen. Der Betroffene ist in diesem Fall die Person, deren Daten erfasst werden sollen. Der Umgang beinhaltet die Speicherung, die Veränderung, die Übermittlung, die Sperrung und das Löschen von Informationen. Die Nutzung umfasst jede Verwendung der Daten, die nicht Bestandteil der Verarbeitung ist.

Die Radio Frequenz Identifikation ist jedoch nicht grundsätzlich ein Problem für den Datenschutz. Ein RFID-Tag der ohne personengebundene Daten verwendet wird, fällt nicht unter das BDSG. Erst wenn der eindeutige RFID-Tag Code mit personenbezogenen Daten verknüpft oder personenbezogene Daten auf dem Tag gespeichert werden, befindet man sich im Anwendungsbereich des BDSG. Um nicht ungewollt Fehler zu begehen und um die notwendigen rechtlichen Grundlagen einzuhalten, sollten folgende Dinge beachten werden:

4.3.1.3. Das Verbot mit Erlaubnisvorbehalt

Das Kapitel 4.3.1.2 zeigte, dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur dann rechtens ist, wenn der Betroffene der Erfassung zugestimmt

[6] Urteil vom 12.04.2005 - 2 BvR 581/01, MMR 2005, 371.
[7] §1 Abs.1 BDSG

hat. Nach §4 Abs. 1 des BDSG [8] gibt es außer der Erlaubnis des Betroffenen noch die Möglichkeit, dass eine andere Rechtsvorschrift vorliegt. Ein Vertragsverhältnis oder die Wahrung berechtigter Interessen sind Beispiele dafür.

Der Träger des RFID-Tags muss der Sammlung seiner Bewegungsdaten zustimmen, bevor diese aufgezeichnet werden dürfen. Dies muss schriftlich geschehen, am Besten bei der Aushändigung des RFID-Tags. Wird die Erlaubnis verweigert, müsste z.B. im Falle eines Angestellten überprüft werden, ob ein Erhebung dieser Daten einem zu erfüllenden Geschäftszweck unterliegt. Dann wäre es auch ohne eine schriftliche Zustimmung möglich.

4.3.1.4. Transparenz

Wenn die beobachtete Person selbst über ihre Daten entscheiden können soll, muss gewährleistet sein, dass sie ausreichend über den Einsatz und der Verwendungszweck der Datenerfassung informiert ist. Der Betroffene hat außerdem das Recht auf Offenlegung der über ihn gespeicherten Daten. Im Zuge der Aufklärung muss der Träger also über die Erfassung informiert werden. Das heißt, er erfährt das er beobachtet wird, für welchen Zweck er beobachtet wird und welche Daten erfasst werden. Weiterhin muss gewährleistet sein, dass es möglich ist die Daten des Trägers separat anzuzeigen, um sie im Fall der gewünschten Offenlegung vorweisen zu können. Die Vorschriften dazu schreiben keine Frist dafür vor, aber es muss die Möglichkeit geben.

Davon ausgehend, dass die vom RFID Tracking betroffenen Personen immer ausreichend über den Zweck der Datenerfassung informiert sind, ist das Hauptproblem die Offenlegung. In großen Systemen kann es durchaus problematisch sein, wenn Daten an verschiedenen Orten oder Datenbanken gesichert sind. Der Punkt der Offenlegung muss somit von Beginn der Planung und Umsetzung der Datenbank beachtet werden. Es muss in einem angemessenen Zeitrahmen möglich sein, die Informationen der gewünschten Person zu finden und zu extrahieren.

4.3.1.5. Zweckbindung

Mit der Zweckbindung schreibt der Gesetzgeber vor, dass die erhobenen Daten nur zu dem im Vorfeld festgelegten Zweck, und nur wie durch den Betroffenen autorisiert, verwendet werden. Eine Speicherung von Daten auf Vorrat, ohne klaren Verwendungszweck, verstößt daher gegen das Datenschutzgesetz [39, Seite 211].

Die verschiedenen Datenschutzgesetze wie Zweckbindung, Datensparsamkeit und andere, sind schwer zu kontrollieren. Es bedarf einer intensiven Prüfung, um festzustellen ob der Anspruch an die Zweckbindung erfüllt ist. Dies ist für Außenstehende nur schwer zu kontrollieren, wodurch die Versuchung entstehen könnte, Daten auch für andere Zwecke zu verwenden. Die Gefahren bei einem solchen widerrechtlichen Vorgehen sind vielfältig. Von den gesetzlichen Strafen einmal abgesehen, bedingt ein öffentlich gewordener Verstoß gleichzeitig einen Vertrauensverlust. Eine vernünftige Planung schützt, wenn sie von vorn herein mit überwachenden Datenschutzorganisationen zusammenarbeitet oder einen unabhängigen Datenschutzbeauftragten ernennt, der z.B. die Einhaltung der Zweckbindung kontrolliert.

4.3.1.6. Erforderlichkeit

Im Umgang mit personenbezogenen Daten, wird durch das Datenschutzgesetz nicht nur die Zweckbindung, sondern auch die Erforderlichkeit verlangt. Dies bedeutet, dass lediglich die Daten erhoben und verarbeitet werden dürfen, die zur Erfüllung der gestellten Aufgabe nötig sind. Es werden für die Auswertung der Trackingdaten also nur die Informationen herangezogen, die zur Erfüllung der Aufgabenstellung notwendig sind.

Auch hier gilt, dass die Kontrolle der Erforderlichkeit schwer ist. Bei einem Verstoß gegen das Datenschutzgesetz drohen gerichtliche Strafen. Deshalb sollte im Vorfeld ausgeschlossen sein, dass widerrechtlich Daten erhoben werden. Auch bei der Erforderlichkeit gilt, dass die datenerhebende Institution ausreichende Möglichkeiten zum Schutz vor Missbrauch einplanen muss.

4.3.1.7. Datensparsamkeit

Einher mit der Erforderlichkeit sollte normalerweise immer auch der datenvermeidende und datensparsame Umgang mit personenbezogenen Daten gehen. Da die Erforderlichkeit und Datensparsamkeit auseinander hervorgehen, sind die Folgerungen für Beide ähnlich. Je weniger personenbezogenen Daten erhoben werden, desto weniger Probleme können aufkommen. Die Erhebung von nicht notwendigen Daten sollte daher auch gänzlich unterbleiben.

Auch hier gilt ähnlich wie bei der Erforderlichkeit, dass die Forderungen nur durch Selbstkontrolle erfüllt werden können. Je nach Komplexität des Systems wird zwar die Prüfung schwieriger, aber wie oben beschrieben, ist Vorsicht geboten. Geeignete Mittel zur Selbstkontrolle sollten auch hier angewendet werden.

4.3.1.8. Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Um nicht von den Möglichkeiten der Technik überrascht zu werden, wird versucht den Einsatz von RFID-Technologien bereits im Vorfeld zu regeln. So beschlossen der Bund und die Länder 2006 auf der 72. Konferenz der Datenschutzbeauftragten verschiedene Punkte [12]. Einige davon wurden bereits im Zuge des BDSG erwähnt, andere dagegen haben dort keine direkte Entsprechung. So fordern die Datenschutzbeauftragten neben der bereits erwähnten Transparenz unter anderem die Kennzeichnung von RFID-Tags und Lesegeräten. Die Kommunikationsvorgänge mit den Chips sollten für den Anwender sichtbar sein, um eine heimliche Anwendung auszuschließen. Das Verbot der heimliche Profilbildung ist ein weiterer Punk, der gefordert wird. Die Konferenz hält als einen weiteren Punkt die „Vermeidung der unbefugten Kenntnisnahme“ fest. Er besagt, dass sichergestellt werden muss, dass niemand unerlaubt Zugang zu den gespeicherten Daten erhält. Mehr dazu im Kapitel 4.3.2. Der letzte Punkte der Liste, die Möglichkeit zur Deaktivierung von Tags, bezieht sich eher auf den Einsatz im Handel, als auf ein ge-

schlossenes System, in dem die RFID-Tags am Ausgang wieder eingesammelt und damit vom bisherigen Träger entfernt werden.

Die Datenschutzbestimmungen werden demnach auch weiterhin den technischen Gegebenheiten angepasst. Die Beachtung der geltenden Gesetze ist nicht nur Mittel zur Vertrauensbildung, sondern durchaus wichtig zur Vermeidung von Datenschutzverstößen.

4.3.2. Maßnahmen zur Sicherung der Datenschutzes

Nachdem die notwendigen Datenschutzgesetze bekannt sind, muss sichergestellt werden, dass sie eingehalten werden beziehungsweise nicht von Dritten umgangen werden können. Auch dies ist Bestandteil des BDSG. Eines der wichtigsten Abschnitte zur Wahrung des Datenschutzes ist der §9, der besagt, dass technische und organisatorische Maßnahmen zu treffen sind, um die erforderliche Sicherheit nach dem Datenschutzgesetz und speziell nach der Anlage zu §9[8] zu gewährleisten. Diese listet die wichtigsten Maßnahmen auf, die zur Sicherung von personenbezogener Daten angegeben werden sollten.

1. **Zutrittskontrolle:** Unbefugten den Zugang zu Datenverarbeitungsanlagen verwehren.

2. **Zugangskontrolle:** Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

3. **Zugriffskontrolle:** Gewährleisten, dass nur Daten genutzt werden, für die der Nutzer eine Berechtigung hat und das personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

4. **Weitergabekontrolle:** Sicherstellen, dass personenbezogene Daten bei einer elektronische Übertragung, beim Transport oder bei der Speicherung auf dem Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und

[8] Anlage (zu §9 Satz 1) im BDSG

das festgestellt werden kann welche Einrichtungen zur Übertragung von personenbezogenen Daten vorgesehen sind.

5. **Eingabekontrolle:** Es muss möglich sein im Nachhinein festzustellen, wer welche Daten im Datenverarbeitungssystem eingegeben, verändert oder entfernt hat.

6. **Auftragskontrolle:** Gewährleistet, dass im Auftrag verarbeitete personenbezogene Daten, nur entsprechend des Auftrages verarbeitet werden können

7. **Verfügbarkeitskontrolle:** Sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

8. **Verarbeitungskontrolle** Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden können.

Diese acht Punkte sollen sicherstellen, dass Systeme und Verarbeitungsprozesse zur Erfassung und Nutzung von personenbezogenen Daten, die gegebenen Datenschutzgesetze einhalten und die Sicherheit dieser Daten gewährleistet können.

Die Umsetzung dieser Punkte ist sehr vom ausgewählten System und seiner Beschaffenheit abhängig. So lassen sich geschlossene Systeme eher sichern als ein offenes System. Diese haben den Anspruch, über verschiedene Netzwerke oder das Internet hinweg zu funktionieren. Es können aber ein paar allgemeine Hinweise gegeben werden. So reicht ein sicher und funktionierendes Benutzersystem mit Authentifizierung aus, um die ersten Punkte wie Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle und Eingabekontrolle zu erfüllen. Eine externe Prüfung durch eine Datenschutzbehörde, der Prozess zum Erwerb eines Datenschutz-Gütesiegels oder die Ernennung eines Datenschutzbeauftragten stellen sicher, das die relativ schwierig zu sichernde Auftragskontrolle und die getrennte Verarbeitung von unterschiedlichen Daten, ebenfalls Beachtung finden. Die Ansprüche an die Verfügbarkeitskontrolle lässt sich in modernen technischen Systemen relativ leicht erfüllen. Jedes gute Datenbanksystem läuft auf redundant gesicherten Datenträgern und stellt so eine verlustfreie Aufbewahrung sicher. Die Weitergabekontrolle kann durch Methoden gewährleistet werden, die im Teil zur Datensicherheit (Kapitel 4.4) beschrieben

werden. Denn die Weitergabekontrolle ist thematisch eng verwandt mit den Gefahren, die durch gezielte Angriffe entstehen, dem Belauschen von Kommunikationsvorgängen entsprechen oder dem unbefugten Zugriff auf personenbezogenen Daten nahe kommen.

4.3.3. Einschätzung

Das Kapitel 4.3 gibt einen Überblick darüber, welche Rolle der Datenschutz bei der Ortung und Verfolgung von Personen mittels RFID spielt. Es sollte offensichtlich sein, dass der Datenschutz und besonders der Schutz von personenbezogener Daten, in Deutschland eine sichere rechtliche Grundlage besitzt. Auch zukünftige Technologien finden dabei regelmäßig Einzug in das BDSG (Siehe Abschnitt 4.3.1.8). Es ist also bereits bei der Planung eines Systems wichtig, dass bei der Erfassung und Verarbeitung von personenbezogene Daten darauf geachtet wird, dass zum Beispiel die acht Punkte aus Abschnitt 4.3.2, Beachtung finden. Dabei ist es erst einmal unerheblich, ob diese Daten mittels RFID oder einer anderen Methode gesammelt werden. Grundsätzlich gibt es keine Einwände und keine rechtlichen Hindernisse gegen die Erfassung und Verarbeitung personenbezogener Daten. Dennoch muss der rechtlich korrekte Umgang mit den Daten streng kontrolliert und das Einverständnis der beobachteten Personen vorhanden sein. Stimmt das Verhalten im Umgang mit den persönlichen Daten, stellt der Datenschutz keine Hürde dar.

In einem Krankenhaus ist es von Bedeutung und von Vorteil, dass die Daten in einem geschlossenes System erhoben werden. Krankenhäuser stellen zwar komplexe Systeme dar, sind aber nach außen weitgehend abgeschlossen. Durch den Umgang mit Patientendaten sind diese Einrichtungen sowieso bestrebt, die Sicherheit der Daten und deren Vertraulichkeit zu gewährleisten. Erfassungssysteme in Handel und Logistik müssen dagegen offen angelegt werden, da die Informationen für andere Stellen zugänglich sein müssen [27, Seite 14 f]. Das nicht öffentlich zugängliche System in einem Krankenhaus, ist leichter zu sichern als ein Netzwerk, dass viele Schnittstellen zu anderen Netzen besitzt. Dort lassen sich die personenbezogene Daten sicherer handhaben, was einigen Da-

tenschutzbestimmungen wie Zutritts-, Zugangs- und Zugriffskontrollen entgegenkommt. Mit möglichen Sicherheitsmaßnahmen, befasst sich das nachfolgende Kapitel 4.4

4.4. Datensicherheit

Dieses Kapitel beschäftigt sich mit den Gefahren und den Maßnahmen zur Datensicherheit im Bezug auf die Kontaktlose Radio Frequenz Identifikation. Die Einschränkung erfolgt deshalb, da es umfangreiche Literatur und Konzepte zur Sicherung der angebundenen Datenbanken gibt. Sie erstrecken sich von Verschlüsselungen für Datenbanken, verschiedenste Zugriffskontrollsysteme oder Methoden zur sicheren Übertragung von Daten. Die Gefahren die durch unerlaubtes Abhören der Radioübertragungen, dem Täuschen von Lesegeräten und Tags oder zum Beispiel auch durch die Störung von Kommunikation entstehen, sind Inhalt dieses Kapitels.

4.4.1. Gefahren

Die Gefahren für die Sicherheit und die Integrität eines Systems, das RFID nutzt sind vielfältig. Vom Abhören, über das Fälschen von ID's, dem Stören und Verändern von RFID-Tags, gibt es die verschiedensten Bedrohungen [9, Seite 15 ff.]. Nicht alle Bedrohungen beruhen einzig und alleine darauf, dass Daten gestohlen oder unbefugt ausgelesen werden. Auch das Stören des normalen Betriebes und die damit verhinderte normale Nutzung stellen eine Gefahr dar. Die Abbildung 4.3 stellt die möglichen Arten der Manipulation dar. Der erste Angriffspunkt ist die Funkübertragung, über welche die Kommunikation zwischen Lesegerät und RFID-Tag erfolgt. Weiterhin gibt es die Bedrohungen für das Lesegerät sowie für den Tag selbst. Welche Gefahren das im Detail sind, soll im folgenden erörtert werden.

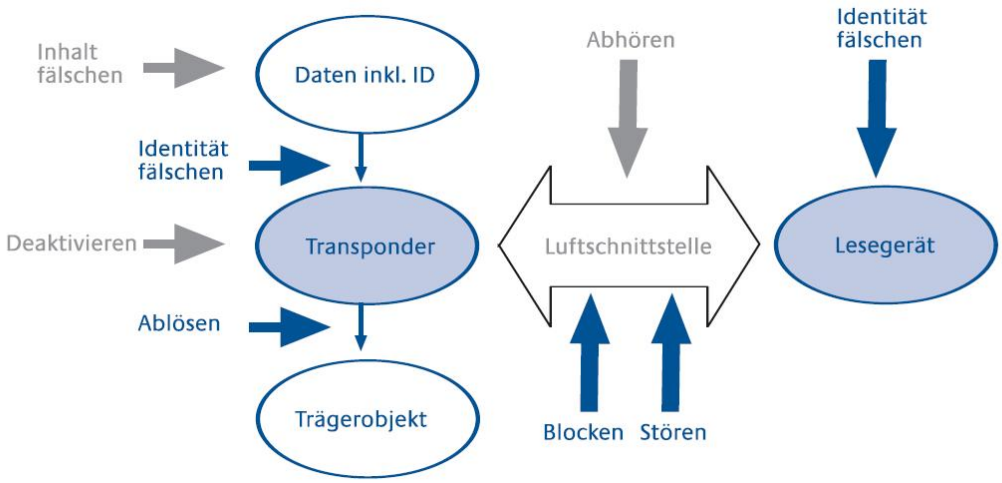


Abbildung 4.3.: Angriffsarten [7, Seite 41]

4.4.1.1. Gefahren bei der Übertragung

Betrachten wir zunächst die Luftschnittstelle in der Abbildung. Hier werden entweder Daten abgehört, oder es wird versucht die Übertragung zwischen Lesegerät und RFID-Tag zu blocken oder zu stören. Das Abhören der Kommunikation stellt sich zwar als möglich, aber auch als technisch schwierig heraus. Denn die Reichweite von passiven Tags ist stark begrenzt und der Kommunikationsvorgang auch nicht in beide Richtungen gleich gut abzuhören. So ist die Übertragung vom Tag zum Lesegerät deutlich schwächer als die ausgehende Kommunikation vom Lesegerät. Theoretisch ist nur das Mithören über die fünffache Entfernung, des maximalen Leseabstandes, vom Tag zum Lesegerät technisch realisierbar [7, Seite 55]. Dies führt bei passiven Tags, mit einer geplant kurzen Lesereichweite, zu einer relativ hohen Sicherheit gegenüber unbefugten Mithörern [7, Seite 55]. Denn normale Überlagerungen und Störungen machen es noch schwieriger, das Signal über große Entfernungen abzuhören. Aber nicht nur das unerlaubte Mithören, sondern auch das Stören oder Blockieren der Übermittlung sind als Bedrohung für die Sicherheit der Daten anzusehen. So gibt es Blockertags, die Lesegeräte überlasten und damit ein gezieltes Erfassen unmöglich machen, oder Störsender, die sämtliche Kommunikation

massiv stören. Im Gegensatz zu Blockertags, sind Störsender zwar verboten, halten aber einen Gewillten nicht von deren Einsatz ab.

4.4.1.2. Gefahren für RFID-Tags

Die Gefahren für einen RFID-Tag hängen stark davon ab, ob der Tag selber Daten speichert oder lediglich die eigene Tag-ID enthält. Denn Daten die auf einem Tag gespeichert werden, sind potentiell gefährdet. Die RFID-Tags haben meist keine Sicherheitsvorkehrungen aufgrund ihrer geringen Rechenleistung. So lassen sich die Informationen auf dem Tag nur unzureichend oder gar nicht verschlüsseln. Aktive Tags sind zwar eher in der Lage Verschlüsselungstechniken auf ihre Daten und ihre Kommunikation anzuwenden, durch die erhöhte Sendeleistung sind sie aber auch über weitere Strecken abhörbar, was das erste genannte Risiko wieder erhöht.

Zwei weitere Punkte, welche die Sicherheit eines RFID Systemes und die Integrität einzelner Tags gefährdet, sind die Vorgänge des Duplizieren und des Emulieren. Beim Duplizieren werden die Informationen eines Tags ausgelesen und auf einen anderen unbeschriebenen Tag gebracht. Dadurch lässt sich das Vorhandensein des zugeordneten Objektes vortäuschen. Das Emulieren funktioniert ähnlich, nur das hier kein neuer Tag beschreiben wird, sondern ein Gerät die gegebenen Informationen bei Bedarf an das Lesegerät übermittelt und so das Vorhandensein des entsprechenden Tags vortäuscht. Duplizieren und Emulieren sind gefährlich, weil es damit möglich ist das Vorhandensein eines bestimmten Objektes vorzutäuschen. Wird zum Beispiel ein mit einem RFID-Tag versehender Gegenstand aus einem Warenkreislauf entnommen, um ihn zu stehlen, kann an seiner Stelle ein duplizierten Tag platziert werden, der das Vorhandensein des Originales vortäuscht.

Eine simple Methode, die Funktion eines RFID-Tags zu sabotieren, ist ihn von seinem dazugehörigen Objekt zu trennen und einem Neuen zuzuordnen. Bei einem Einsatzzweck zur Ortung, kann dies durch das Liegenlassen von Tags oder Vertauschen geschehen. Auch unabsichtliches Liegenlassen kann die Datenerfassung verfälschen. Dazu kommen

die aktiven Vorgänge, bei dem die Transponder mit Absicht abgelöst werden. Eine weitere Methode RFID-Tags in ihrer Funktion zu stören, ist den Tag selbst außer Gefecht zu setzen. Er kann physisch zerstört werden, in dem der Tag von seiner Antenne getrennt oder einer sehr hohen Feldeinwirkung aussetzt wird. Außerdem kann versucht werden, das Kill-Kommando von RFID-Tags zu missbrauchen. Dieses aus Datenschutzgründen eingebettete Kommando eines Tags, deaktiviert ihn unwiderruflich. Sollte der Vorgang eine Authentifizierung erfordern, wie bei aktuellen Tags bereits Standard, ist diese Art von Missbrauch allerdings unwahrscheinlich.

4.4.1.3. Gefahren für Lesegeräte

Es gibt noch weitere Bedrohungen, die zum Beispiel von falschen Lesegeräten ausgehen, deren Identität gefälscht oder vorgetäuscht wird. Verfügt ein Tag beziehungsweise die Kommunikation zwischen RFID-Tag und Lesegerät über keine Verfahren zur Authentifizierung der Gegenstelle, ist es leicht die gespeicherten Daten auszulesen oder Daten auf den RFID-Tags zu verändern. Ohne Authentifizierung ist das größte zu überwindende Problem die Mindestreichweite des RFID-Tags [7]. Aber auch zum vortäuschen der möglichen Authentifizierung gibt es Methoden, wie den Man-in-the-middle- oder die Replay-Attacke. Dies sind nur ein paar von einer ganzen Reihe möglicher Angriffsarten. Eine genauere Darstellung möglicher Angriffsarten, ist bereits in anderen Quellen sehr ausführlich dargestellt worden. Informationen dazu sind zum Beispiel in [9, Seite 15 ff] aufgeführt.

4.4.2. Sicherheitsmaßnahmen

Bei allen Bedrohungen für die Daten und die Funktion eines RFID Erfassungssystems, gibt es natürlich auch vielfältige Möglichkeiten sich zu schützen. Die erste und einfachste Art sich vor unbefugtem Zugriff auf seine Daten zu schützen, ist es diese nicht auf den RFID-Tags zu speichern. Auf den Tags selbst, sollte nur die eigene Identifikationsnummer gespeichert sein. Alle zusätzlichen Informationen, werden unabhängig und lokal getrennt

davon gespeichert. Der Einsatz einer Datenbank bietet sich auch in diesem Fall an. Denn zum eine Datenbank besitzt weniger Angriffsmöglichkeiten. Risikofaktoren wie sie bei der Radio Frequenz Identifikation und der Datenübertragung durch die Luft entstehen, fallen oftmals weg. Die Sicherungssysteme für die Authentifizierung, den Zugriffsschutz oder den Integritätsschutz einer Datenbank sind erprobt, leichter umzusetzen und auch sicherer [27, Seite 41].

Damit bleibt als einzige brauchbare Information, die Identifikationsnummer auf dem Tag übrig. Ist diese für einen RFID-Tag immer gleich, so könnte auch sie von Dritten verwendet werden, um unbemerkt Bewegungsdaten und Trackinginformationen zu erhalten. Die Gefahr, dass anhand eines eindeutigen Merkmals unbemerkt ein Bewegungsprofil erstellen werden kann, wird durch jede zugängliche und gleichbleibende Information, wie z.B. der Tag-ID, größer. Verhindern lässt sich dies durch die Verwendung von Meta-IDs [9]. Diese sind nicht statisch sondern werden dynamisch nach bestimmten Kriterien generiert. Die kann auf verschiedene Art und Weisen erfolgen. Beispiele dafür sind der Randomized-Hash-Lock oder das Chained-Hash-Verfahren. Die RFID-Tags dafür, müssen zumindest Hash Werte berechnen und teilweise auch Zufallszahlen generieren können. Diese Funktionen sind aktuell noch nicht auf allen RFID Tags vorhanden, gehören aber zu den Standards der nächsten Versionen. Über die Hash-Verfahren wird erreicht, dass die eigentliche ID mithilfe einer Zufallszahl oder einer dem Lesegerät bekannten, anderen Hash-ID, umgewandelt wird. Dadurch werden bei jeder Übertragung unterschiedliche Meta-IDs versandt, die dann zurückgerechnet werden. Sicherheitstechnisch schwierig ist dabei lediglich der Austausch des Hash-Schlüssels. Aber auch dies lässt sich mit aufwendigeren Verfahren sicher gestalten.

Zu den in Zukunft standardmäßig eingebauten Funktionen [39, Seite 263 f] gehören auch Verfahren zur Authentifizierung. Den Missbrauch des Kill-Befehles, Duplizierungen und Emulationen oder das unautorisierte Auslesen von Tag-Daten werden durch eine sichere Authentifizierung verhindert. Die genannten Verfahren für die Meta-IDs, arbeiten ebenfalls nur, wenn sich Lesegerät und RFID-Tag gegenseitig authentifizieren. Nur dann lassen sich die Meta-IDs auflösen. Die Variante, die Authentifizierung über den Austausch

eines Passwortes zu regeln, ist die einfachste und lässt sich auch mit Tags ohne erweiterte kryptografische Funktionen betreiben. Das Problem dabei ist, ähnlich wie bei der Übertragung der Meta-IDs, die Verteilung der Passwörter auf die Tags und die Übertragung eines Zufallswertes zwischen Lesegerät und Tag. Die Verteilung der Passwörter auf die Tags muss geschehen bevor die RFID-Tags verwendet werden, und es muss dem Lesegerät ebenfalls im Vorfeld bekannt sein. Wichtig dabei ist, dass jene Passwort nicht über die Luftschnittstelle übertragen werden. In einem relativ kleinen geschlossenen System wie in unserem Beispielkrankenhaus, ist das jedoch weniger ein Problem, da jeder RFID-Tag einzeln vorbereitet werden kann. Wenn es dann zur Authentifizierung kommen soll, sendet das Lesegerät zum Beispiel eine Zufallszahl oder einen Zeitstempel. Dieser Wert wird mit Hilfe des Passwortes verschlüsselt und zurück übertragen. Dort angekommen entschlüsselt das Lesegerät den übertragenen Authentifizierungscode mit Hilfe des ihm bekannten Passwortes. ISt der errechnete Wert gleich dem Gesendeten, war das Passwort richtig und der RFID-Tag ist authentifiziert. Für eine gegenseitige Authentifizierung muss der RFID-Tag die gleiche Prozedur vollführen, weswegen der ein Zufallsgenerator und die erweiterten kryptografischen Fähigkeiten auf den RFID-Tags nötig sind. Es soll angemerkt werden, dass eine Authentifizierung nach dem eben beschriebenen Challenge-Response Verfahren aufwendig ist. Durch die zusätzlichen Fähigkeiten sind die erweiterten RFID-Tags im Moment teurer als die ohne Kryptografiefähigkeiten.

Bei aller Datensicherheit, können einige Methoden die als Gefahr für die Datensicherheit gelten, auch zu ihrem Schutz verwendet werden. Zum einen Blockertags, die genutzt werden um Leseversuche von außen zu blockieren und zumindest bestimmte nicht verwendete Adressbereiche zu blockieren. Das ist aber weder zuverlässig noch ratsam. Weiterhin gibt es die dauerhaft Deaktivierung durch Trennen von Antenne und Tag und die Nutzung des kill-Befehls um RFID-Tags nach dem Beenden ihrer gestellten Aufgabe sicher zu deaktivieren. Damit wäre eine weitere unbefugte Nutzung, der durch ihn repräsentierten Informationen, unmöglich.

4.4.3. Einschätzung

Die wichtigsten Mittel zur Vermeidung der Gefahren für die Datensicherheit, liegen sowohl in verbesserter Technik also auch im Vermeiden von möglichen Gefahrensituationen. Ein geschlossenes System ist zwar sicher, aber ein Krankenhaus hat höhere Anforderungen an die Sicherheit, da hier sensible Daten verarbeitet werden. Grundsätzlich wird festgestellt, dass die Möglichkeiten zum Schutz der Datensicherheit im Gegensatz zum Datenschutz eher technischer Natur sind und so bei den Entwicklern von RFID-Lesegeräten und Tags liegen. Durch richtige Planung können große Risiken vermieden werden. Weitere Schutzmaßnahmen hängen von der richtigen Wahl der Hardware und den damit möglichen Optionen zur Verschlüsselung und Authentifizierung ab. Auf jeden Fall sollte davon abgesehen werden, die Daten auf den Tags lediglich mit Passwörtern zu sichern. Die Informationen zum Aufenthaltsort einer Person [39, Seite 250], ist allein des Datenschutzes wegen zu sichern. In einer Umgebung wie einem Krankenhaus, sollte sichergestellt sein, dass solch sensible Daten sicher verwaltet werden. Authentifizierungs- und Verschlüsselungsverfahren sind als Mittel zum Schutzes daher zwingend erforderlich.

Da hier kein offenes weltweites System zur Verfolgung von Personen geplant wird, sondern ein geschlossenes räumliches begrenztes Trackingsystem, dass mit personenbezogenen Daten arbeitet sollten die folgenden Punkte beachtet werden. Daten sollten nicht auf den RFID-Tags gespeichert, sondern in einer gesicherten Datenbank, die alle Informationen enthält. Dieser Schritt vermeidet von vornherein weitere Probleme, die mit dem möglichen Ausspionieren von Daten einhergehen. Weiterhin sollte die Reichweite der Lesegeräte so gering wie möglich gehalten werden. Dadurch wird vermieden, dass Daten über längere Strecken gesendet werden als eigentlich benötigt. Die kurze Reichweite erschwert so Dritten das Mit- und Abhören der Kommunikation zwischen RFID-Tag und Lesegerät. Die Vereinbarung von kurzen Timeout-Zeiten beim Lesen von RFID-Tags, kann helfen Angriffe zu erschweren, bei denen die Kommunikation abgehört und gefälscht wird (Replay-Angriffe, Man-in-the-middle)[9, Seite 23]. Wird zusätzlich noch, durch Authentifizierung zwischen Tag und Lesegeräten und durch die Verschlüsselung der

Tag-IDs, die Beobachtung von spezifischen Informationen einzelner Tags erschwert, sind die größten Gefahren beseitigt. Einen all umfassenden Schutz wird es auch dann nicht geben, wenn alle Punkte beachtet wurden. Der technische und rechnerische Aufwand diese Sicherheitsvorkehrungen zu umgehen, ist dann sehr hoch und nicht mehr einfach durch Laien zu umgehen [7, Seite 54].

5. Simulation eines RFID-Trackingsystems

Dieses Kapitel widmet sich der Umsetzung der RFID Anywhere Umgebung zur Simulation eines RFID-Netzwerkes und den Möglichkeiten der weiteren Verwertung der daraus resultierenden Ortsinformationen für Patientenworkflows. Dazu werden in den folgenden Unterkapiteln die theoretischen Vorüberlegungen für die Simulation behandelt. Zuerst wird die Umsetzung und die Anzeige der Simulation und der gewonnenen Daten beschrieben. Danach folgt ein Ausblick auf die Möglichkeiten die Daten anzuzeigen, zu verarbeiten oder weiter zu verwenden .

5.1. Aufbau und Planung

Die Grundlage der gesamten Simulation des RFID Netzwerkes stellt, wie bereits in Kapitel 2.5 dargestellt, das RFID Anywhere Framework von Sybase dar. Diese System ermöglicht es eine beliebiges Setup von RFID-Lesegeräten und RFID-Tags zu simulieren, ohne reale Hardware verwenden zu müssen. Des weiteren beinhaltet das Paket natürlich noch viel mehr Möglichkeiten der Weiterverarbeitung und Behandlung der gewonnenen Informationen. Zunächst geht es aber um den theoretischen Aufbau der Simulation und um die Beschreibung einiger Entscheidungen, die den Aufbau und das Design der Simulation beeinflusst haben.

5.1.1. Räumliche Aufteilung und Anordnung der Lesegeräte

Mit Hilfe von RFID Anywhere ist es möglich, ein kleines theoretisches Modell einer Patientenaufnahme zu entwerfen. Darin wird es 4 Räume geben, den Empfang, den Warteraum, das Untersuchungszimmer und das Arztzimmer. Jeder Bereich besitzt eine Verbindung zu einem oder mehreren anderen Bereichen (bezeichnet mit E, EW, AW, UW), wie in Abbildung 5.1 zu erkennen ist. Die Verbindungen oder Durchgänge zwischen den Räumen sollen mit Lesegeräten versehen sein, die jeden RFID-Tag erfassen würden, der sich für einen Raumwechsel in den Lesebereich begibt. Dadurch ist es möglich, die räumlichen Änderungen des Aufenthaltsortes der RFID-Tags und ihrer Träger zu erfassen.

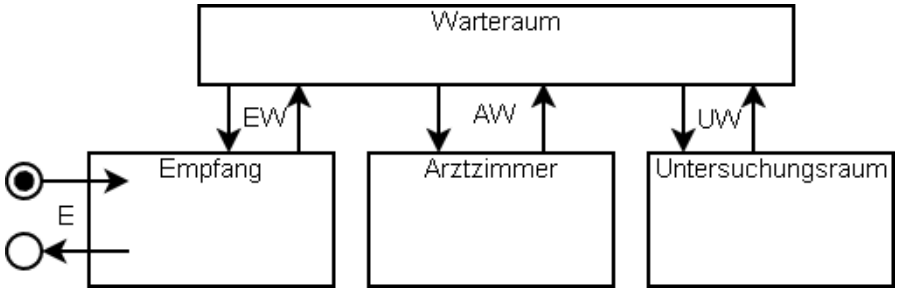


Abbildung 5.1.: Skizze des Raumplanes der Simulation

Warum werden aber lediglich die Durchgänge erfasst? Bei der Planung eines RFID-Trackingsystemes, wurden im Vorfeld verschiedene Ansätze erläutert. RFID-Tags werden direkt geortet, indem mit mehrere Lesegeräte über Triangulation die ungefähre Position im Verhältnis zu den Lesegeräten berechnet wird. Da die Simulation nicht die Ortungstechnologien simulieren soll, sondern die Möglichkeiten der Auswertung der Ortsinformationen. So ist es ausreichend zu wissen in welchem festgelegtem Bereich sich der Patient aufhält und daraus abzuleiten, welcher Tätigkiet er nachgeht. Der Zweck des Aufenthaltes ist in diesem Fall direkt vom Ort ableitbar. Es reicht dafür zu wissen in welchem Raum sich der Träger des RFID-Tags befindet. Wenn diese Information genug ist, reicht es aus sämtliche Ein- und Ausgänge zu den Bereichen zu überwachen, da Räume normalerweise nur darüber zu betreten oder zu verlassen sind. Die einzige Schwierigkeit

besteht darin festzustellen, in welche Richtung der Patient den Raum verlässt. Wird ein Lesegerät auf jeder Seite einer Tür installiert, könnte auch die Richtung der Bewegung ermittelt werden. Sind die Lesebereiche so gewählt das sie sich nicht überschneiden, kann der zeitliche Versatz gemessen werden. Das Lesegerät, das den Tag zuerst erfasst bestimmt die Richtung aus der er kommt. Der zweite Lesevorgang bestätigt die Richtung in die er geht. Für die Simulation und Situation reicht es aus, wenn wir uns auf ein einfaches Modell beschränken. Es wird pro Durchgang nur ein Lesegerät simuliert. Das ganze Modell ist so angelegt, dass jeder Durchgang nur aus einem Raum in genau einen Anderen führt. Dadurch wird, bei Kenntnis des bisherigen Aufenthaltsortes, der dazugehörige neue Aufenthaltsort geschlussfolgert. Ein Wechsel vom „Untersuchungraum“ direkt in das „Arztzimmer“ ist deswegen nicht möglich. Er muss durch die Lesegeräte (UW) und (AW) und damit durch den Warteraum laufen.

Ein Beispiel: Das Lesegerät (AW) aus Abbildung 5.1 erfasst einen RFID-Tag und stellt nun fest, dass dieser zu Patient X gehört. Das Lesegerät (AW) überwacht den Durchgang zwischen dem Warteraum und dem Arztzimmer. Befindet sich der Patient X bereits in einem der beiden Räume, kann in unserem abstrakten Fall davon ausgegangen werden, dass er in den Raum geht, in dem er sich bisher nicht befunden hat. In unserem Modell gehen wir davon aus, dass Patienten sich nicht entschließen, innerhalb der Reichweite des Lesegeräts umzukehren. Denn dies würde bedeuten, dass der Patient in dem Raum bleibt, indem er ist und die Auswertung ihn fälschlicherweise dem neuen Raum zuordnet.

Es ist gewollt, dass das gesamte System der Simulation nur über den Ein- und Ausgang am Empfang (E) betreten oder verlassen werden kann. Für unsere Simulation bedeutet dies, dass wir jeweils komplette Pfade bewerten können. In der Realität wäre der Ein- und Ausgang gleichzusetzen mit der Registrierung des RFID-Tags auf einen Patienten und dem abschließenden Deaktivieren des RFID-Tags, wenn der Patient das Krankenhaus verlässt. Außerdem erfüllt diese Einschränkung einen weiteren Zweck. Das hier vorgestellte System ist geschlossen, was bedeutet, dass es in dieser Simulation nicht möglich ist, dass ein RFID-Tag aus dem Nichts erscheint. Nur über den Eingang direkt am Start, kommen Elemente hinzu. Dort wird er als neu registriert und die Aufzeichnung der Be-

wegungsinformationen beginnt.

Soweit zum Aufbau des Modells. Der Vorteil der Vereinfachungen ist, dass hiermit Details bei der Implementierung der Simulation vernachlässigt werden können, die rein technischer Natur sind und die Auswertung der Bewegungsdaten nicht direkt betreffen. So sind Bewegungsrichtungen leicht technisch zu ermitteln und dann auch auszuwerten. Lesefehler oder das plötzliche Auftauchen von RFID-Tags im System sollte immer auch in einer realen Umgebung vermieden werden. Allerdings arbeiten die Ortungssystem mit einer sehr hohen Zuverlässigkeit, solange alle Antennen und Lesegeräte korrekt konfiguriert und ausgerichtet sind.

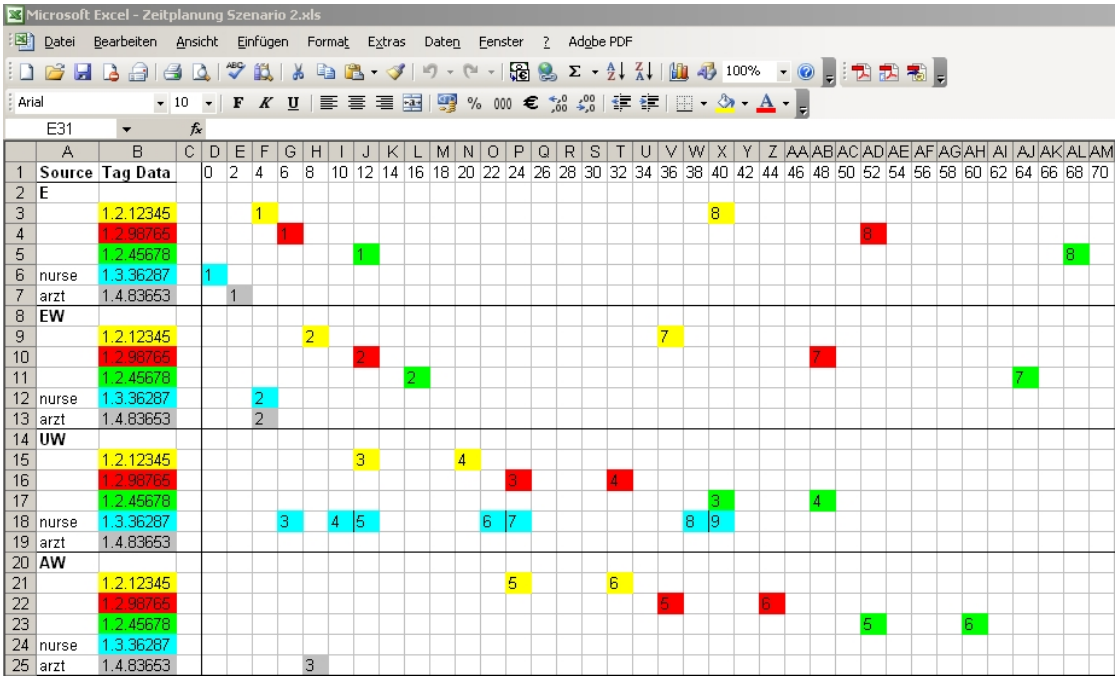
5.1.2. Simulationsdaten

Nachdem bekannt ist, wie die Simulationsumgebung aussehen soll, muss diese natürlich noch mit simulierten Personen und ihren Kodierungen im RFID-Tag Format gefüllt werden. Dies geschieht durch Simulationsdateien, die mit Hilfe des in Kapitel 2.5 erwähnten Simulator Data Editor (Abb. 5.3) erstellt werden.

5.1.2.1. Vorbereitung der Simulationsdaten

Als erstes muss die Grundlage der Simulation geschaffen werden. Mittels des mitgelieferten Editor für die Simulationsdaten, wird das Auftreten der RFID-Tags festgelegt. Für jedes Lesegerät wird einzeln, das Auftreten und Auslesen der RFID-Tags erstellt. Bei 4 Lesegeräten werden 4 Simulationsdateien erstellt, jeweils eine für die Lesegeräte mit den Bezeichnungen E, EW, AW und UW. In diesen ist jeweils festgelegt, welcher Tag, zu welcher Zeit mit welcher ID erkannt wird. Jede dieser Dateien wird nun mit den Zeitpunkten gefüllt, zu denen ein oder mehrere RFID-Tags erkannt werden sollen. Da mindestens 4 verschiedene RFID-Tags simuliert werden, ist die Planung wichtig. Um Fehler zu vermeiden, wird ein Ablaufplan über das Auftreten der RFID-Tags erstellt. Dies erfolgte der Übersicht halber einfach als Zeitdiagramm, welches als Ausschnitt in Abbildung 5.2 zu

sehen ist. Abgebildet ist die Zeiteinteilung in den einzelnen Spalten. Die Zeilen stellen die einzelnen Tags für das jeweilige Lesegerät dar. Mit Hilfe dieser Planung können die Simulationsdateien einfach und schnell erstellt werden. Ohne eine entsprechende Planung können bei der Vielzahl an Events schnell Fehler entstehen.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM
1	**Source**	**Tag Data**		0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64	66	68	70
2	**E**																																						
3		1.2.12345				1																		8															
4		1.2.98765					1																							8									
5		1.2.45678								1																												8		
6	nurse	1.3.36287		1																																			
7	arzt	1.4.83653			1																																		
8	**EW**																																						
9		1.2.12345						2														7																	
10		1.2.98765								2																		7											
11		1.2.45678										2																								7				
12	nurse	1.3.36287				2																																	
13	arzt	1.4.83653				2																																	
14	**UW**																																						
15		1.2.12345								3				4																									
16		1.2.98765														3				4																			
17		1.2.45678																						3				4											
18	nurse	1.3.36287					3		4	5					6	7							8	9															
19	arzt	1.4.83653																																					
20	**AW**																																						
21		1.2.12345														5				6																			
22		1.2.98765																				5				6													
23		1.2.45678																												5				6					
24	nurse	1.3.36287																																					
25	arzt	1.4.83653						3																															

Abbildung 5.2.: Zeitverlauf der simulierten RFID-Tags

5.1.2.2. Kodierung der Tags für die Simulation

Die EPCglobal arbeitet bereits offiziell an Standards für den Gesundheitsbereich, allerdings gibt es noch keine eindeutige Festlegung dafür. Daher wird in dieser Simulation zunächst kein bestehender EPC verwendet, sondern die RFID-Tag IDs frei vergeben. Dabei beachtet werden dafür die gängigen und in Kapitel 4.2.1 beschriebenen Kodierungsvorgaben. Eine Einschränkung gibt es dabei. Bisher ist es nur möglich, EPC konforme IDs zu vergeben. Ein alternativer Standard, wie der ISO eHIBC, wird nicht unterstützt. Als Codierung wird die GID (Siehe Kapitel 4.2.1) gewählt. Der GID-96 setzt sich aus 3 Bereichen zusammen die eine eindeutige Identifizierung ermöglichen. Diese 3 Bereiche

werden wie folgt gefüllt. Für die *General Manager Number* wird immer die 1 vergeben. Die *Object Class* erhält je nach Typ eine andere Zahl. Die *Serial Number* wird dann für jeden RFID-Tag einzeln eindeutig festgelegt. Eine Übersicht zur genauen Umsetzung der einzelnen Teile der Kodierung findet sich im Anhang in der Tabelle C.1.

Im Falle einer konkreten Realisierung könnten die Strukturen natürlich mit entsprechend sinnvollen und eindeutigen Daten gefüllt werden. Da wäre die Codierung des Krankenhauses oder der Abteilung innerhalb der *General Manager Number*. Der Personen- oder Gerätetyp oder z.B. die aktuelle Jahreszahl ließe sich als *Object Class* kodieren und die Patientenidentifikationsnummer (PIN) als *Serial Number*. Da sie in Krankenhäusern mit elektronischem Krankenhausinformationssystem oft vorhanden sind [34, Seite 494], liegt diese Möglichkeit Nahe. Die Möglichkeiten der EPC Vergabe sind also entsprechend weitläufig und ermöglichen eine individuelle Konfiguration je nach Wunsch.

Nach diesen Vorgaben ist eine Kodierung für einen Patienten die „1“ für die General Manager Number, die Object Class Nummer „2“ und die eindeutigen Patientenidentifikationsnummer „12345“ als Serial Number. Das Ergebnis ist für einen GID-96 EPC zusammengesetzt der folgende Schlüssel: 350000001000002000003039

Diese Zahl ist hexadezimal kodiert und erleichtert die Darstellung. Die Hexadezimalwerte 35 0000001 000002 000003039 ergeben dann in eine EPC konforme lesbare Schreibweise umgewandelt folgendes: urn:epc:pat:gid-96:1.2.12345. Die genaue Zusammensetzung des URN-Codes ist in dem Abschnitt 4.2.1.2 dargestellt.

5.1.2.3. Umsetzen im Simulator Data Editor

Da der Ablauf erstellt ist und die Kodierung der RFID-Tags feststeht, kann nun festgelegt werden, zu welchen Zeitpunkten sie genau auftreten..

Das Schema wird dazu in den RFID Simulator Data Editor übertragen. Das geschieht, indem zuerst eine Gruppe anlegt wird (siehe Abbildung 5.3), die einen beliebigen Zeitpunkt beschreibt. Der Name für diese Gruppe sollte so gewählt sein, dass es möglich

ist, aus ihm den ungefähren Zeitpunkt zu Schlussfolgern. In diesem Fall beinhaltet der Gruppenname den Zeitpunkt des Auftretens. Innerhalb der Gruppe werden alle Tags festgelegt, die zu dem Zeitpunkt sichtbar sein sollen. Es könnten beliebig viele Tags sichtbar gemacht werden, allerdings sollen in diesem Beispiel nie mehr als zwei RFID-Tags gleichzeitig durch einen simulierten Reader erkannt werden. Denn praktisch wird es kaum vorkommen, dass mehr als eine Person gleichzeitig durch eine Tür geht .

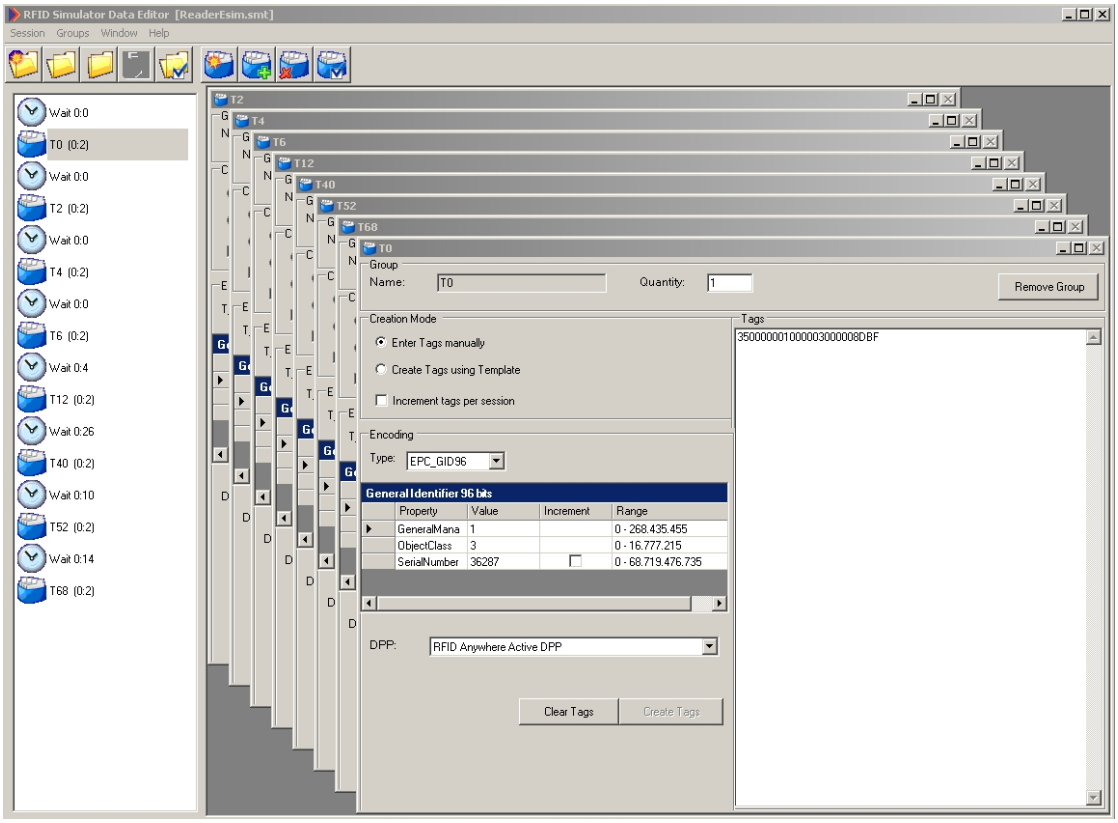


Abbildung 5.3.: Screenshot der Simulationsdatei für das Lesegerät E im RFID Simulator Data Editor

Sind die Tags angelegt, wird der genaue Zeitpunkt bestimmt, zu dem diese Gruppe erscheinen soll. Der Startzeitpunkt lässt sich festlegen, indem angegeben wird, wie viele Sekunden seit dem Erkennen der vorherigen Gruppe vergangen sind und wie lange sich die Tags „im Lesebereich des Readers“ befinden. Bei der derzeitig vorliegenden Version des Editor ist zu beachten, dass es nicht möglich ist Zeiten nachträglich einzufügen. Die Angabe der Gruppen muss chronologisch erfolgen. Bei Änderungen im zeitlichen

Ablauf, müsste die Datei neu erstellt werden. Die Zeitangabe erfolgt, indem die Zahl der vergangenen Sekunden angegeben wird. Es wird kein Zeitpunkt angegeben, sondern die x vergangenen Sekunden seit erscheinen eines Vorgängers.

Nach dem Festlegen des Namens, der später als Bezeichnung für den RFID Multiprotocol Simulator verwendet wird, kann zusätzlich die Zahl der Wiederholungen der Simualtionsdaten festgelegt werden. Sind für alle 4 Lesegeräte Simulationsdateien angelegt worden, können sie eingebunden werden.

5.1.2.4. Einbinden in RFID Anywhere

Um die Simulationsdateien zu nutzen, müssen sie importiert werden. Dies geschieht über die Administratorkonsole (Siehe Abb. 5.4). Über das *Session Data* Feld, wird eine Datei als *RFID Multiprotocol Simulator* (siehe Abb. 2.7) eingelesen. Durch diesen Schritt werden die virtuellen Lesegeräte initialisiert. Dieses simulierte Lesegerät „entdeckt“ im laufenden Betrieb nun zu den festgelegten Zeiten die RFID-Tags.

5.2. Umsetzung der Simulation

Das nachfolgende Kapitel beschreibt die Implementierung der funktionellen Bestandteile der Simulation. Die beinhaltet die Erstellung eines Business Moduls in dem Daten gesammelt und weitergeleitet werden und den Entwurf und die Implementierung eines grafischen Interfaces. Darauf folgt die Beschreibung der möglichen Weiterverarbeitung der gewonnen Daten.

5.2.1. Implementierung des Business Moduls

Sind die simulierten Lesegeräte eingerichtet und Funktionsfähig, müssen die Informationen daraus weiterverarbeitet werden. Dazu werden verschiedene Möglichkeiten angeboten, die aufkommenden Daten zu verarbeiten. Zum einem erfolgt dies über die bekannten

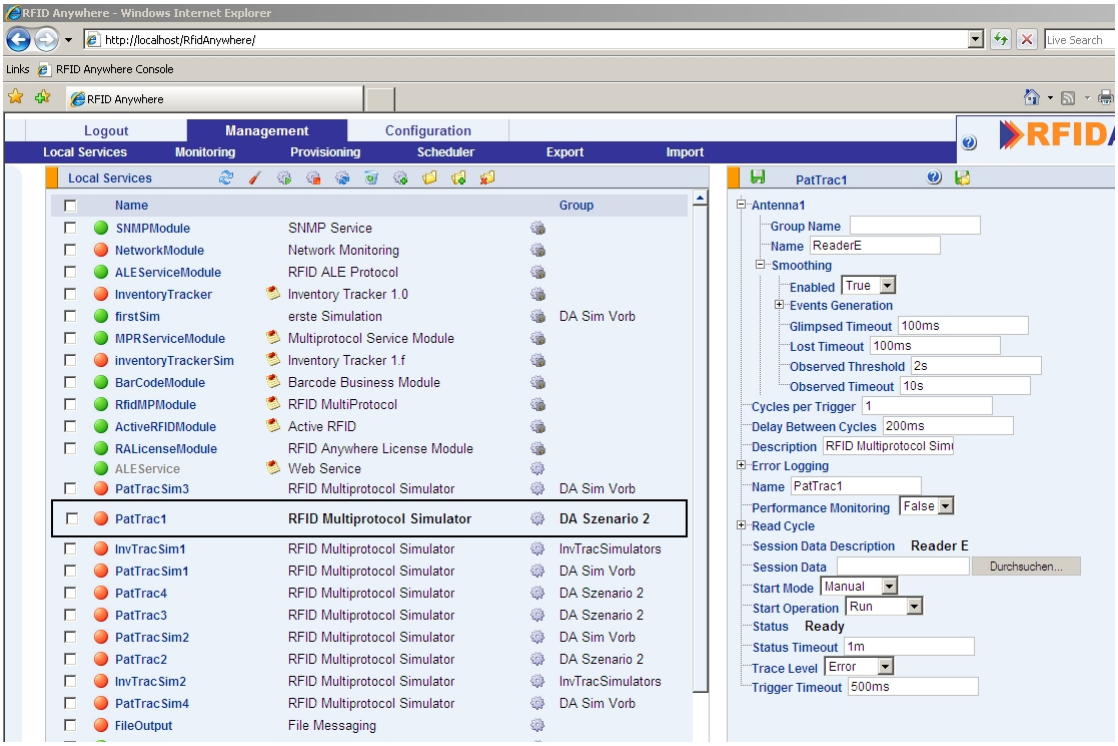


Abbildung 5.4.: Screenshot der Administratorkonsole

Module *RFID ALE Business Module* oder die *Multiprotocol Service Module*. Diese Varianten verarbeiten die Daten und geben sie je nach Wunsch gefiltert weiter. Genaueres dazu kann in Kapitel 2.5 nachgelesen werden. Die andere Möglichkeit sind die Business Module (BM). Diese Module werden als Service in das Framework von RFID Anywhere geladen. Während die ALE und die Multiprotocol Engine kaum Möglichkeiten bieten die Daten zu modifizieren, bietet ein BM eine Vielzahl von Möglichkeiten. Geschrieben für die .NET Plattform, lassen sich diese Module als Service in das RFID Anywhere System integrieren. Das zu entwickelnde Business Modul basiert auf den im Developers Guide [29] vorgestellten Informationen und der als Beispiel mitgelieferten Implementierung der Inventory Tracker Demo von RFID Anywhere. Um die Möglichkeiten des RFID Anywhere Frameworks zu nutzen wurden die integrierten Funktionen wie die Subscriberlist, die interne FireXML Funktion oder die SecondarySources Liste verwendet. Die Subscriberlist beinhaltet die Empfänger für die umgewandelten Informationen. Diese lassen sich in der Administratorkonsole festlegen. Die FireXML Funktion ist eine Funktion,

mit der die verarbeiteten Daten in XML Form an die Empfänger aus der Subscriberlist geschickt werden. Über die SecondarySources lassen sich während der Bearbeitung zusätzliche Daten integrieren. Sie enthält z.B. die echten Namen zu Tag-IDs, oder deren genauen Typ. Die Vielfältigkeit der Verarbeitung beruht darauf, dass das Business Modul in C# geschrieben ist. Durch die Verwendung der vollwertigen Programmiersprache, sind alle angebotenen Funktionen in vollem Umfang für das Business Modul nutzbar.

5.2.1.1. Funktionsweise

Die Module agieren mit der RFID-Hardware, egal ob simuliert oder real existierend, über Controller. Diese Controller vermitteln die Informationen zwischen der möglichen Hardware und den Business Modulen. Dadurch sind die Module, die für RFID Anywhere geschrieben sind, unabhängig vom Typ und vom Standard, mit dem die Hardware arbeitet.

Zum leichteren Verständnis ist das Sequenzdiagramm des BM in der Abbildung 5.5 dargestellt. Darauf sind drei Klassen zu erkennen, die den groben Aufbau des Moduls erläutern. Die erste Klasse ist die Abbildung des RFID Anywhere Systems. Da es keine exakten Angaben zur internen Funktionsweise von RFID Anywhere gib, wurde die Darstellung als einzelnes Element gewählt. Dies soll das Gesamtsystem darstellen, das z.B. nach Start einer Simulation das entsprechende BM startet oder die entstehenden Daten weiterschickt.

Das erstellen eines Controllers (5), ist der erste Schritt auf dem Weg die Informationen der RFID-Tags zu erhalten. Die drei Funktionen zu Beginn (1-3) erstellen beim Starten die notwendigen Felder für das Webinterface zur Steuerung des Moduls. Der Controller wird darauf hin initialisiert und an das entsprechende vorliegende BM gebunden. RFID Anywhere ruft dazu immer die Start() Methode (4) auf, die daraufhin mittels StartControllers() (5) alle Controller aktiviert, dem BM zuweist und den Container zur Speicherung der Daten anlegt (6). Nachdem das BM an den Controller gebunden ist, werden die dazugehörigen RFID Lesegeräte gestartet. Der Lesevorgang währt solange, bis

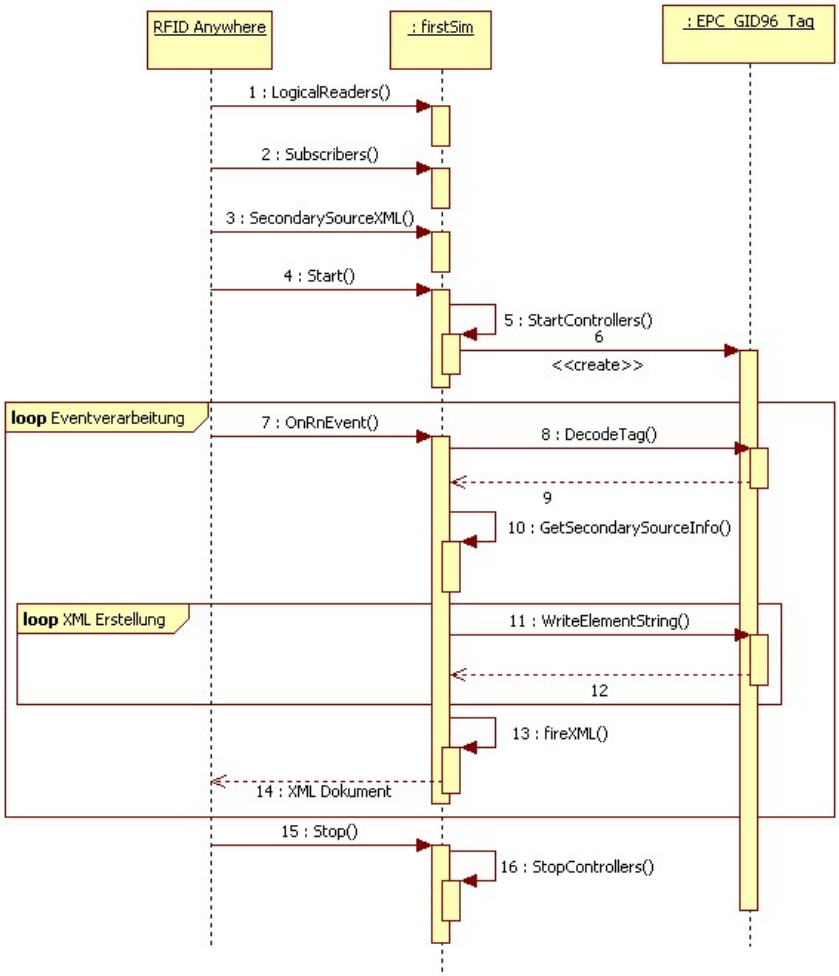


Abbildung 5.5.: Sequenzdiagramm des RFID Anywhere Business Moduls für die Simulation

eine Stop() Funktion diesen wieder beendet. Kommt es nun zu einem Readerevent, also zu einem Ereignis, welches das auftreten oder verschwinden eines Tags anzeigt, so wird vom System die OnRnEvent (7) Funktion aufgerufen. Diese muss im BM implementiert sein, um die Informationen des Lesegerätes zu erhalten. Innerhalb dieser Schleife werden die Informationen dekodiert (8) und mit zusätzlichen Informationen hinterlegt (10). Liegen alle Informationen vor, kann der eigentliche Informationsträger zusammengestellt werden. Dazu ruft die WriteElementString() Funktion (11) die einzelnen Informationen nach und nach aus dem Container zur Speicherung ab (12). Ist dies beendet, wird die

nun erstellte XML Datei an die FireXML (13) Funktion übergeben. Sie sendet die Daten (14) an die Connectoren in der Subscriberliste (2). Die Subscriber übertragen die Daten dann je nach ihrer individuellen Konfiguration weiter (Siehe Abbildung 2.7). Die OnRnEvent Funktion wird solange wiederholt, bis die Stop() Funktion (15) über den StopControllers() (16) Aufruf, den Zugriff auf den Controller beendet. Damit stellt das BM seine Arbeit ein.

Mit diesem Aufbau ist es möglich, die Funktionen des RFID Anywhere Frameworks vollständig zu nutzen. Es ermöglicht weiter modular Lesegeräte hinzuzufügen, zusätzliche Informationen einzubinden und die resultierenden Informationen an die verschiedenen Module zu versenden. Die Konfiguration der eben genannten Funktionen erfolgt dabei auch über die RFID Anywhere Konsole. Für die Simulation einer RFID Umgebung wäre dies wichtig, da diese so flexibel bleibt. Wenn Lesegeräte oder Empfänger getauscht werden, müssen diese lediglich neu in das Webinterface des BM eingetragen werden. Es aber genauso möglich, die funktionalen Elemente fest zu integrieren und die Bearbeitung der Events und Informationen in einem extra Programm ablaufen zu lassen. In diesem Fall wurde zum Testen der Funktionen des Frameworks darauf verzichtet. Da die Anzeige und die Auswertung der Daten nicht Bestandteil des Frameworks sind, wurden diese zusätzlich in einem davon unabhängigen externen Programm umgesetzt (Siehe 5.2.2).

Die Verbreitung der Daten erfolgt in dieser Simulation über das Netzwerk. Die FireXML Funktion stellt die übergebenen Daten, in der erstellten XML Form, den in der Subscriberliste eingetragenen Empfängern bereit. Einer dieser Empfänger ist der *TCP messaging connector*. Er ermöglicht es, RFID Anywhere Inhalte mittels TCP Protokoll an externe Anwendungen zu senden. Dafür wird eine IP für den TCP Konnektor benötigt und einen Port auf dem dieser arbeitet [30, Seite 121 ff]. Danach ist es möglich über diese Schnittstelle alle Informationen die das BM produziert über das angeschlossene Netzwerk abzurufen. Genauso wäre es natürlich möglich die Verbreitung über das Internet zu realisieren, die Daten in einer Datenbank zu speichern oder die Informationen lokal in Textdateien abzulegen.

5.2.2. Das Java Demo GUI

Die Bearbeitung und Weiterverarbeitung der RFID Events (das Auftreten der RFID-Tags) obliegt vollständig dem in das RFID Anywhere integriertem BM. Funktionen, die das anzeigen von Daten ermöglicht, sind nicht in das Framework integriert. Da dieses nicht das Ziel des Frameworks ist, werden sie in einem extra Programmteil behandelt. Sämtliche relevanten Daten sind bereits durch das BM erfasst und aufbereitet, so dass es jetzt noch nötig ist, diese aus dem TCP/IP Stream zu lesen. Das BM verbreitet die in XML-Form vorliegenden Daten kontinuierlich über das Netzwerk. Um diese zu erhalten und zu speichern, muss dann eine Verbindung zum Port der angegebenen IP des BM hergestellt werden.

Wie bereits angesprochen, besteht die Hauptaufgabe des in Java geschriebenen grafischen Benutzeroberfläche (GUI) darin, anzuzeigen was RFID Anywhere an Informationen versendet. Eine Übersicht über die Funktionsweise der GUI findet sich in der Grafik 5.6. Dies ist eine vereinfachte Darstellung der Abläufe. Sie steht beispielhaft für die kompletten Vorgänge. Das Diagramm beinhaltet z.B. eine vereinfachte Behandlung der Speziallfälle und der genauen Darstellung.

Nach dem Start, dem Initialisieren des XMLAssetManagers (2) und dem Start der grafischen Elemente, beginnt die Behandlung der empfangenen Daten. Dabei kommen Threads zum Einsatz, um die Verarbeitungsgeschwindigkeit zu erhöhen. Threads können parallel nebeneinander abgearbeitet werden und ermöglichen es dadurch, dass Funktionen oder Methoden sich nicht bei der Abarbeitung gegenseitig blockieren. Da die Abfolge der RFID Events nicht vorhersehbar oder regelmäßig ist, müssen diese Ereignissen ohne Verlust ausgewertet werden können. In diesem Fall wird jede eintreffende XML aus dem Inputstream des Netzwerkes als einzelner Thread behandelt. Um die Daten des Inpustreams zu empfangen wird ein Socket angelegt, der als Schnittstelle zwischen dem Programm und dem Netzwerkprotokoll fungiert. Dazu wird nur der Port benötigt, auf denen der Socket nach dem Datenstrom suchen soll.

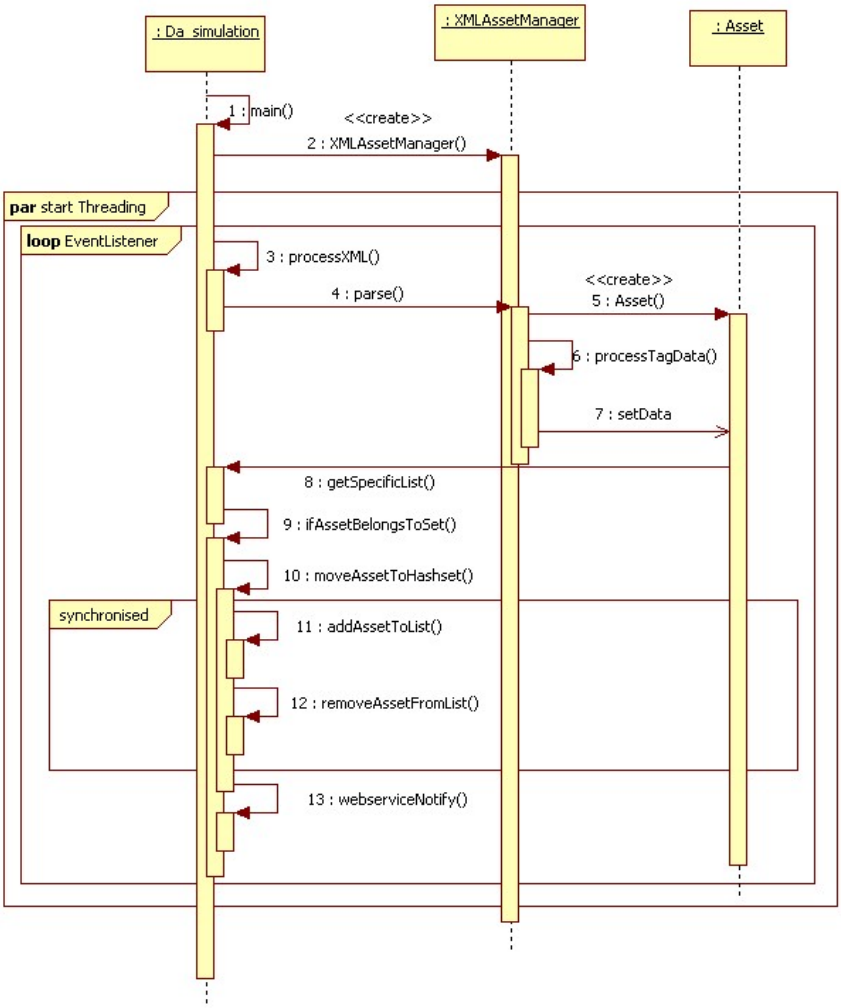


Abbildung 5.6.: Sequenzdiagramm der Java Demo GUI

Von nun an beginnt das Programm auf eintreffende Nachrichten zu warten. Wird eine Nachricht empfangen, beginnt die eigentliche Verarbeitung. Die processXML() Funktion (3) übergibt den Inputstream an den dafür definierten Contenthandler der XMLAsset-Manger Klasse. Der Contenthandler wird über die parse() Funktion (4) aufgerufen und beginnt mit der Verarbeitung. Ein Container zur Speicherung der Informationen wird angelegt (5) und der Inputstream auf seine möglichen XML Elemente hin untersucht (6). Der SAX XML Parser der dabei zum Einsatz kommt, sucht nach XML Elementen. Entdeckt er ein XML Tag schreibt er dessen enthaltenden Informationen einzeln in

den Asset Container. Die setData Methode (7) ist hier eine Zusammenfassung der einzelnen Schreibvorgänge für die Objekt-ID (ID), den Typ (TYPE), die Referenznummer (REF), die Quelleninformation (Source) und die Zeit (Time). Sind die Daten komplett ausgewertet und im Asset Container gespeichert, wird dieser über den Funktionsaufruf getSpecificList() (8) an die Hauptklasse zurückgegeben. Von nun an wird die Verarbeitung wieder in der DA_simulation Klasse ausgeführt.

Zuerst wird überprüft, von welchem Lesegerät das Ereignis stammt. Die Funktion ifAssetBelongsToSet() (9) liest die Source Information aus, um festzustellen, an welchem Lesegerät der RFID-Tag erkannt wurde. Wenn das Lesegerät der Rezeption erkannt wurde, wird dieser entweder neu zu einer Raumliste hinzugefügt oder aber aus dem System entfernt, je nachdem ob er sich schon im Raum befunden hat oder nicht. Ansonsten erfolgt die Untersuchung durch die moveAssetToHashset() Funktion (10) die prüft, in welchem Raum sich der RFID-Tag vorher befunden hat. Da ein Lesegerät wie bereits in Abschnitt 5.1.1 erwähnt, immer zwei Räume verbindet, muss nur geprüft werden, in welchem Abschnitt er sich bereits befunden hat. Die nächsten Abläufe sind durch ein „synchronized“ gekennzeichnet. Das bedeutet, dass der Zugriff auf die Listen mit den Tags nur sequenziell erfolgen darf. Dies soll gleichzeitige Zugriffe auf die Listen verhindern. Denn die Elemente müssen, wenn sie erkannt wurden, noch aus der alten Liste entfernt (12) und in die neue Liste geschrieben werden (11). Damit es bei den Schreibvorgängen nicht zu unabsichtlichen Überschreibungen innerhalb der Listen durch andere Threads kommt, wird der Zugriff auf diese so beschränkt. Sind die Änderungen die durch die Ereignisse ausgelöst worden sind durchgeführt, erfolgt als letztes der Versand der Informationen zu den Änderungen per Webservice an den Workfloweditor (13). Hier endet die Bearbeitung eines Threads. Sollten weitere Informationen empfangen werden, wird dafür ein neuer Thread gestartet.

5.2.3. Optionen zur Datenverarbeitung und Speicherung

Die vorab vorgestellte Demo GUI speichert die Daten nicht selber. Da sie nur zur Anzeige und Weiterleitung gedacht war, muss die Speicherung anderweitig erfolgen. Grundsätzlich ist es aber das selbe Prinzip. RFID Anywhere versendet die vorher verarbeiteten Daten an eine seiner Messaging Connector Schnittstellen. Diese Schnittstellen können beliebig abgefragt werden. So wäre als Empfänger der Daten nicht nur die DEMO GUI denkbar, sondern auch eine beliebige Datenbank mit einer entsprechenden TCP Schnittstelle. Damit könnten die Daten zunächst einmal gespeichert und später ausgewertet werden. Genauso wäre es möglich sie direkt in verschiedene Log Dateien zu sichern, von denen lediglich der Speicherort bekannt sein muss. Auch hier erfolgt die Auswertung im Nachhinein. Die Demo GUI hat gezeigt, dass die Liveanzeige der Daten funktioniert. Die Datenspeicherung erfolgt in diesem Fall noch zusätzlich über den Umweg des Workfloweditors. Diese Methode wurde getestet, da die ursprüngliche Idee aus der Erfassung der Patientenpfade mittels des erwähnten Workfloweditors erfolgte. Dabei kommuniziert die Demo GUI mit der vorher definierten Webservice Schnittstelle der Client-Server Version des Workfloweditors [11]. Die Speicherung der Daten erfolgt dann nach der im Anhang D aufgeführten XSD Struktur.

Genauso ist es möglich, die Vorverarbeitung nicht durch das RFID Anywhere Business Modul vollziehen zu lassen. In diesem Fall kommen die Daten ungefiltert und im vollen Umfang bei den ausgewählten Messaging Connectoren an, wo sie abgerufen oder gespeichert werden können. Dabei besteht jedoch die Gefahr, dass zuviele unnötige Daten ausgegeben werden und die auswertenden Programme damit überfordert werden. Von daher ist es in den meisten Szenarien sinnvoll die gewünschten Daten nach bestimmten Kriterien direkt durch die RFID Middleware filtern oder zusammenfassen zu lassen. Das erspart Speicherplatz und verhindert Überlastungen durch ein zu große Menge von Daten.

5.3. Auswertung

Die Auswertung der Daten kann bei dieser Form der Erfassung auf zwei Arten erfolgen. Sie können direkt weiterverarbeitet werden oder erst einmal gespeichert. Je nach Einsatzzweck unterscheiden sich die Ziele und die Anforderungen. Die direkte Weiterverarbeitung würde für die Liveanzeige und Übertragung von Werte oder für die direkte Ortung von Objekten genutzt werden. So können Informationen live erfasst werden. Als Beispiel dafür kann der bereits mehrfach angesprochene Workfloweditor genannt werden. Er empfängt die Daten der Simulation, könnte dann in einem realen RFID-Netzwerk genauso Informationen von echten Patienten empfangen, aufzeichnen und speichern. Zu seiner Benutzung sind Hinweise im Anhang E festgehalten.

Bei dem zweiten Szenario erfolgt die Speicherung zunächst einmal in einer Datenbank. Die Daten lassen sich langfristig speichern und werden erst im Nachhinein zur Auswertung herangezogen. Hierdurch wird es möglich, Daten miteinander zu kombinieren und so für statistische Analysen zu verwenden. Welche Einsatzzwecke sind dabei denkbar? Einige Möglichkeiten wären Effizienzmessungen mit denen die Auslastung von verschiedenen Entitäten gemessen werden könnte. Es wäre möglich zu überprüfen, ob z.B. das eingesetzte Personal durchgehend ausgelastet ist. Das wäre ein Hinweis darauf, dieses zu verstärken, wenn sich zeitgleich viele Patienten auf einen Termin mit den betroffenen Personen warten. Umgekehrt, kann überprüft werden, wie viele Personen derzeit behandelt werden, um damit die Auslastung des Personals flexibel zu gestalten.

Ein weiterer Punkt wäre der Versuch die Terminvergabe an der Analyse auszurichten. So ließe sich testen, ob sich die persönlichen Erfahrungen und die daraus resultierende Terminpolitik der Mitarbeiter mit den Messungen des Trackingsystems decken. Wenn sich z.B. feststellen ließe, dass es zu bestimmten Zeiten leerer oder voller ist als zu anderen Zeiten, könnte versucht werden über eine geänderte Terminvergabe die Ankünfte der Patienten zu steuern.

Zu einem wirtschaftlich geführten Krankenhaus gehört auch Planungssicherheit. Lassen

sich durchschnittliche Zeiten für Patientenaufenthalte, Behandlungen, Untersuchungen bestimmen, ergäbe dies einen Zugewinn an Informationen für die Administration. Auch wenn sich bestimmte Zahlen wie, die maximale Anzahl gleichzeitiger Patienten oder der Zuwachs bzw. Abschwung bei den Patientenzahlen auch aus den betriebswirtschaftlichen Daten ergeben, ist diese Methode möglicherweise schneller und weniger aufwendig in der Erhebung.

Bei der Optimierung der Abläufe in Krankenhäusern und bei der Behandlung von Patienten kommen verschiedene Werkzeuge, wie klinische Behandlungspfade zum Einsatz (siehe [1]). Patientenworkflows oder die weniger komplexen Patientenpfade, können als Hilfe für die Erstellung von Behandlungspfaden dienen. Mögliche Hinweise auf Abläufe der Behandlungen wären sicher erkennbar. Aber auch später wären Messung einiger Kennzahlen, wie Verweildauer, Zahl von bestimmten Untersuchungen oder Verlegungszeiten möglich.

6. Zusammenfassung

Das Ziel der Evaluierung war es zu überprüfen, in wieweit sich die bestehende RFID-Technologie für den Einsatz zur Erfassung von Patientenworkflows einsetzen lässt. Betrachtet wurden dabei sowohl technische als auch rechtliche Grundlagen. Durch den Einsatz der RFID-Technik in der Industrie ist die Entwicklung im Bereich der passiven und aktiven Tags, sowie der Standardisierung zur Kennzeichnung mittels EPC weit fortgeschritten. Sowohl der EPC als auch der eHIBC, der auf einem barcodbasiertem Kennzeichnungssystem beruht, sind bereits jetzt in der Lage, die umfangreicheren Anforderungen in der Medizintechnik zu gewährleisten. Mit den nächsten Generationen der Standards werden auch zusätzliche Funktionen wie auf den Tags verbaute Verschlüsselungs- und Authentifizierungsmethoden oder ein größerer Speicher für zusätzliche Daten integriert. Zum aktuellen Zeitpunkt ist der eHIBC für den Gesundheitsbereich nach Betrachtung der Recherche besser geeignet, da er frei verfügbar und eindeutiger auf den Medizinbereich ausgerichtet ist.

Bei dem in der Machbarkeitsstudie erörterten rechtlichen Kontext, sind zusammengefasst vor allem im Bereich der personenbezogenen Daten umfassende Auflagen gefordert. So muss gewährleistet sein, das alle beobachteten Personen ihr schriftliches Einverständnis geben haben, über die Erfassung informiert sind und ihre Daten sicher verwahrt werden. Während die Anforderungen an den Datenschutz klar definiert und Mittel zu seiner Einhaltung zur Verfügung stehen, sind die Sicherungs- und Authentifizierungsfähigkeiten der RFID-Tags und Lesegeräte noch kritisch zu bewerten. Dabei ist vor allem die Einführung der im Abschnitt 4.4.2 beschriebenen Sicherheitsmaßnahmen, stark von den jeweiligen

Herstellern abhängig, was den eigenen Einfluss auf die Planung der Sicherheitsaspekte beschränkt.

Wie die Beschreibung vorhandener Trackingsysteme gezeigt hat (Siehe Abschnitt 3), variieren die gewählten Lösungen im Gesundheitsbereich hinsichtlich der Hard- und Softwarekonfiguration stark. Um die dadurch entstehende Bandbreite zu erfassen, wurden in Kapitel 2 die technischen Grundlagen beschrieben um im Kapitel 5 die Simulationssoftware RFID-Anywhere zu evaluieren. Diese ermöglicht es sowohl die RFID-Hardware, als auch die Software zur Weiterverarbeitung zu simulieren. Somit kann die Planung eines Systems vor dem eigentlichen Aufbau exakter und mit mehr Optionen, zum Beispiel für die Wahl der Lesegeräte, erfolgen. Weiterhin ist es möglich verschiedene Arten der Weiterverarbeitung zu testen. Ob als Ausgabe in Dateiform oder als integrierbare Möglichkeit über ein selbst entworfenes Business Modul, das die Daten vorverarbeitet und weiterversendet. Auch die Anbindung einer Datenbank, welche die Informationen zwischenspeichert, ist realisierbar.

Zu der Simulation wurde im Rahmen dieser Arbeit ein grafisches Interface entworfen, um die Erkennung und Weiterverteilung der Daten zu testen. Dieses registriert erfolgreich den Aufenthaltsort der einzelnen RFID-Tags, gemäß der vorher festgelegten Planung. Damit ist gezeigt, dass der Aufbau und die Funktionen eines zu realisierenden RFID-Systems bereits vor seiner Umsetzung testbar ist. Richtig angewandt, lassen sich so Probleme wie sie in [42] beschrieben sind, bereits im Vorfeld ergründen und damit vermeiden.

7. Ausblick

Auf Basis der Ergebnisse dieser Arbeit, sind weitere Untersuchungen denkbar. Es könnte überprüft werden, ob die Portierung der Simulation in den realen Betrieb wirklich so einfach zu bewerkstelligen ist, wie es der Hersteller angibt.

Die Entwicklung von neuen Konzepten zur Nutzung der RFID-Technologie im Krankenhaus wäre eine weiter Aufgabe. Möglich wären dabei, das Auffinden von medizinischen Geräten oder die Überwachung von OP-Räumen. Damit könnte man ebenfalls bestehende Lagersysteme für Arzneimittel und Medikamente integrieren. Der Verbrauch dieser Waren könnte automatisch protokolliert und gleichzeitig dokumentiert werden.

Weiterhin wäre es interessant zu wissen, ob es Kennzahlen gibt, die während des Betriebes interessant für das Krankenhausmanagement wären. So wäre sie unter Umständen in der Lage, Entscheidungen besser, schneller und kostengünstiger zu treffen.

Der letzte Punkt ist die Unterstützung bei der Erstellung und Pflege von Behandlungspfaden. Durch einfache Regeln könnten Schlussfolgerungen hergeleitet werden, die durch den Aufenthaltsort und das beteiligte Krankenhauspersonal den Zweck des Aufenthaltes erschließen könnten.

Bei der richtigen Verwendung wird die Radiofrequenz-Identifikation unsere Möglichkeiten die Welt zu erfassen in Zukunft stark erweitern, immer vorausgesetzt, der vernünftige Umgang mit ihr wächst in gleichem Maße mit.

Literaturverzeichnis

[1] *Deutsche Gesellschaft für klinisches Prozessmanagement e.V.* www.dgkpm.de, (12.11.2008).

[2] Akiyama, Masanori: *Risk Management and Measuring Productivity with POAS - Point of Action System -.* www.ehcca.com/presentations/hitsymposium/akiyama_3.doc, (17.07.2008).

[3] Arndt, Holger: *Supply Chain Management - Optimierung logistischer Prozesse.* Gabler, 3., aktualisierte und überarbeitete auflage Auflage, 2006. http://www.springerlink.com/content/u7w645x102085186/, (27.11.2008).

[4] Berlecon Report: *RFID im Pharma- und Gesundheitssektor - Vision und Realität RFID-basierter Netzwerke für Medikamente.* 2005.

[5] Berthold, Oliver, Prof. Ph.D. Oliver Günther und Dr. Sarah Spiekermann: *RFID: Verbraucherängste und Verbraucherschutz.* http://www.taucis.hu-berlin.de/_download/rfid.pdf, (19.09.2008).

[6] BITKOM Projektgruppe RFID: *BITKOM RFID Guide 2006.*

[7] Bundesamt für Sicherheit in der Informationstechnik, (BSI): *Risiken und Chancen des Einsatzes von RFID-Systemen - Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit.* 2004.

[8] Bundesministeriums der Justiz: *Bundesdatenschutzgesetz*, 2006. http://bundesrecht.juris.de/bdsg_1990/, (01.07.2008).

[9] Bundesministerrium für Bildung und Forschung: *RFID - Studie 2007 - Technologieintegrierte Datensicherheit bei RFID-Systemen.* 2007.

[10] Burgert, O, T Neumuth, M Fischer, G Strauß, A Dietz, J Meixensberger und HU Lemke: *Workflowanalyse und Ontologien für endoskopische NNH-Chirurgie.* 2006. http://www.gmds2006.de/Abstracts/106.pdf, (22.08.2008).

[11] Czygan, Michael: *Konzeption und prototypische Implementierung eines Web Service gestützten Workflow-Aufnahmesystems für chirurgische Abläufe.* Diplomarbeit, Hochschule Mittweida, 2008.

[12] Datenschutzbeauftragten des Bundes und der Länder: *Verbindliche Regelungen für den Einsatz von RFID-Technologien.* In: *72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, 2006.

[13] edition W3C.de: *Die W3C-Spezifikationen in deutscher Übersetzung und Kommentierung.* Technischer Bericht. http://www.edition-w3c.de/, (05.02.2008).

[14] Egan, Marie T. und Warren S. Sandberg: *Auto Identification Technology and Its Impact on Patient Safety in the Operating Room of the Future.* Surgical Innovation, 14(1):41–50, 2007.

[15] EHIBCC: *ISO-RFID eTAG-x - The ISO powered solution for item tracking using RFID Tags in compliance with ISO/IEC standards for Barcode.* EHIBCC, 2004. http://www.hibc.de/Documente/ISO-RFID.pdf, (01.07.2008).

[16] EHIBCC: *Ihr Weg mit Barcode und RFID: Daten am Objekt - die sichere Wahl.* 2007. http://www.hibc.de/startseite_d.htm, (01.07.2008).

[17] EPCglobal, Inc: *EPCglobal Tag Data Standards Version 1.3.1.* http://www.epcglobalinc.org/standards/tds/tds_1_3_1-standard-20070928.pdf, (01.07.2008), 2006.

[18] Finkenzeller, Klaus: *RFID Handbuch.* 2006.

[19] Floerkemeier, Christian: *EPC-Technologie - vom Auto-ID Center zu EPCglobal.* 2004.

[20] Forschungsinstitut für Rationalisierung: *Trusted-RFID - Vertrauenssiegel für RFID-Anwendungen.* http://www.fir.rwth-aachen.de, (18.09.2008).

[21] Goanta, Marcus: *RFID - mögliche Ansätze im Gesundheitswesen.* http://www.ztg-nrw.de/ZTG/content/e35/e612/e3069/lecture_downloads3322/object3328/RFID-mglicheAnstzeimGesundheitswesen_ger.pdf, (10.01.2008), 2006.

[22] GS1 Germany: *EPCglobal Netzwerkkomponenten.* http://www.gs1-germany.de/internet/content/produkte/epcglobal/epc_rfid/epcglobal_netzwerk/komponenten/index_ger.html, (16.08.2008).

[23] GS1 Germany: *RFID-Prozesse/Wirtschaftlichkeit/Hardware.* http://www.gs1-germany.de/internet/content/produkte/epcglobal/epc_rfid_in_der_praxis/rfid_infoboerse/rfid_prozesse/index_ger.html, (06.03.2008).

[24] GS1 Germany: *EPCglobal Inc.* http://www.epcglobal.de/, (05.02.2008), 2008.

[25] GS1 Healthcare: *GS1 Healthcare Newsletter.* 11:5, July 2008.

[26] HIBCC: *Using HIBC Standards with RFID: An Implementation Guideline.* http://www.hibcc.org/AUTOIDUPN/RFID.htm, (01.07.2008), 2007.

[27] Holznagel, Bernd und Mareike Bonnekoh: *RFID - Rechtliche Dimensionen der Radiofrequenz-Identifikation.*

[28] iAnywhere Solutions, Inc: *RFID Anywhere Overview.* http://www.sybase.com/content/1034553/rfidanywhereoverview.pdf, (01.07.2008), 2005.

[29] iAnywhere Solutions, Inc: *RFID Anywhere Developers Guide.* Technischer Bericht, 2007. http://www.ianywhere.com/developer/product_manuals/rfid_anywhere/index.html, (01.07.2008).

[30] iAnywhere Solutions, Inc: *RFID Anywhere Getting Started Guide.* Technischer Bericht, 2007.

[31] IBM Deutschland: *Die Uniklinik in Nizza sorgt dank RFID für optimale Notfallversorgung und gute Besserung.* http://www-05.ibm.com/de/solutions/rfid/rfid_kundenszenarien_gesundheit.html, (25.02.2008).

[32] Informationsforum RIFD e.V.: *RFID im Gesundheitswesen.* 2007. http://www.info-rfid.de/, (27.02.2008).

[33] Lampe, Matthias, Christian Flörkemeier und Stephan Haller: *Einführung in die RFID-Technologie.* 2005.

[34] Lehmann, M. Thomas und Erdmuthe Meyer zu Bexten: *Handbuch der medizinischen Informatik.* Hanser, 2002.

[35] MCKinsey&Company: *Perspektiven der Krankenhausversorgung in Deutschland*, 2006. http://www.mckinsey.de/downloads/presse/2006/060502_bb_praesentation_perspektiven_der_krankenhausversorgung_in_deutschland.pdf, (03.12.2008).

[36] Nahas, Huzaifa Al und Jitender S. Deogun: *Radio Frequency Identification Applications in Smart Hospitals.*

[37] RFID Journal: *Singapore Fights SARS with RFID.* 2003. http://www.rfidjournal.com/article/articleview/446/1/1, (27.02.2008).

[38] RFID-Support-Center: *Logistik-Lexikon.* http://www.logisticsdictionary.com/, (29.01.2008).

[39] TAUCIS: *Technikfolgenabschätzung - Ubiquitäres Computing und Informationelle Selbstbestimmung.* Juli 2006.

[40] Texas Instruments - RFID Systeme. http://www.ti.com/rfid/graphics/productImages/hf-i_lg-rectangle.jpg, (12.11.2008).

[41] Togt, Remko van der, Erik Jan van Lieshout, Reinout Hensbroek, E. Beinat, J. M. Binnekade und P. J. M. Bakker: *Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment.* The Journal of the American Medical Association, 299, 2008. http://jama.ama-assn.org/cgi/content/short/299/24/2884, (29.09.2008).

[42] Wang, Shang Wei, Wun Hwa Chenb, Chorng Shyong Onga, Li Liuc und Yun Wen Chuangb: *RFID applications in hospitals: a case study on a demonstration RFID project in a Taiwan hospital.* 2006.

[43] Weiser, Mark: *The Computer for the Twenty-First Century.* Scientific American, 265:94–104, 1991. http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html, (19.09.2008).

A. XML Beispielaufbau

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
 <wurzel>
      <titel>Inhalt oder Titel</titel>
      <eintrag>
           <stichwort>XML</stichwort>
           <beschreibung>Extensible Markup Language</beschreibung>
      </eintrag>
      <eintrag>
           <stichwort>RFID</stichwort>
           <beschreibung>Radio Frequency Identification</beschreibung>
      </eintrag>
 </wurzel>
```

B. EPC Headers

in der nachfolgenden Tabelle finden Sie eine Übersicht über alle bisher festgelegten EPC Header. Einige von ihnen sind noch reserviert für zukünftige Zwecke während andere nur noch Übergangsweise bis zum Ablauf der alten Spezifikation gelten werden. Danach

Header Value (binary)	**Header Value (hex)**	**Encoding Length (bits)**	**Encoding Scheme**
0000 0000	00	NA	Unprogrammed Tag
0000 0001	01	NA	Reserved for future Use
0000 001x	02,03	NA	Reserved for future Use
0000 01xx	04,05,06,07	NA	Reserved for future Use
0000 1000	08	64	Reserved until 64bit Sunset <SSCC-64>
0000 1001	09	64	Reserved until 64bit Sunset <SGLN-64>
0000 1010	0A	64	Reserved until 64bit Sunset <GRAI-64>
0000 1011	0B	64	Reserved until 64bit Sunset <GIAI-64>
0000 1100 to 0000 1111	0C to 0F		Reserved until 64 bit Sunset Due to 64 bit encoding rule in Gen 1

Tabelle B.1.: Electronic Product Code Header

Header Value (binary)	**Header Value (hex)**	**Encoding Length (bits)**	**Encoding Scheme**
0001 0000	10	NA	Reserved for Future Use
to	to	...	
0010 1110	2E	NA	
0010 1111	2F	96	DoD-96
0011 0000	30	96	SGTIN-96
0011 0001	31	96	SSCC-96
0011 0010	32	96	SGLN-96
0011 0011	33	96	GRAI-96
0011 0100	34	96	GIAI-96
0011 0101	35	96	GID-96
0011 0110	36	198	SGTIN-198
0011 0111	37	170	GRAI-170
0011 1000	38	202	GIAI-202
0011 1001	39	195	SGLN-195
0011 1010	3A		Reserved for future Header values
to	to		
0011 1111	3F		
0100 0000	40		Reserved for future Header values
to	to		
0111 1111	7F		

Tabelle B.1.: Electronic Product Code Header

Header Value (binary)	**Header Value (hex)**	**Encoding Length (bits)**	**Encoding Scheme**
1000 0000 to 1011 1111	80 to BF	64	Reserved until 64 bit Sunset <SGTIN-64> (64 header values)
1100 0000 to 1100 1101	C0 to CD		Reserved until 64 bit Sunset
1100 1110	CE	64	Reserved until 64 bit Sunset <DoD-64>
1100 1111 to 1111 1110	CF to FE		Reserved until 64 bit Sunset
1111 1111	FF	NA	Reserved for future headers longer than 8 bits

Tabelle B.1.: Electronic Product Code Header

Position für die Teilung	Company ID		Objekttyp ID	
	Bits	Stellen	Bits	Stellen
0	40	12	04	01
1	37	11	07	02
2	34	10	10	03
3	30	09	14	04
4	27	08	17	05
5	24	07	20	06
6	20	06	24	07

Tabelle B.2.: Angaben für das Teilungsfeld im EPC Header [17]

C. Kodierung der Simulations-Tag-IDs

In der nachfolgenden Tabelle sind die Werte für die Kodierung der Tag-IDs festgehalten. In der letzten Spalte sind die Werte dann zusammengefasst als Hex-Wert, so wie sie auch auf den Tag gespeichert werden könnten.

Typ	General-Manager-Number	Object-Class-Number	Serial-Number	Tag-ID
Patient	1	2	12345	350000001000002000003039
			98765	3500000010000020000181CD
			45678	350000001000002000B26E
Schwester	1	3	36287	3500000010000030000008DBF
Arzt	1	4	83653	3500000010000040000146C5

Tabelle C.1.: Übersicht der verwendeten RFID-Tag IDs

D. Schema der Workflow-Struktur

Die hier vorgestellte Struktur zur Speicherung von Workflows basiert auf dem Speicherformat des Workfloweditors. Eine genaue Beschreibung ist im Text [11] zu finden.

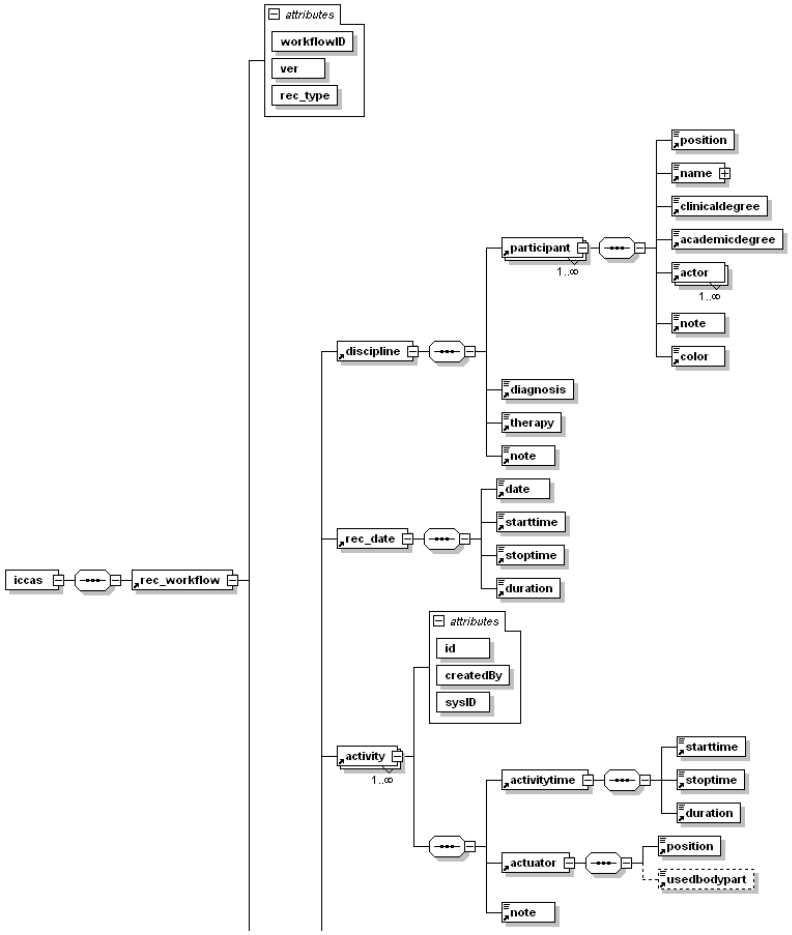


Abbildung D.1.: grafisches Schema der Workflow Struktur - Teil 1

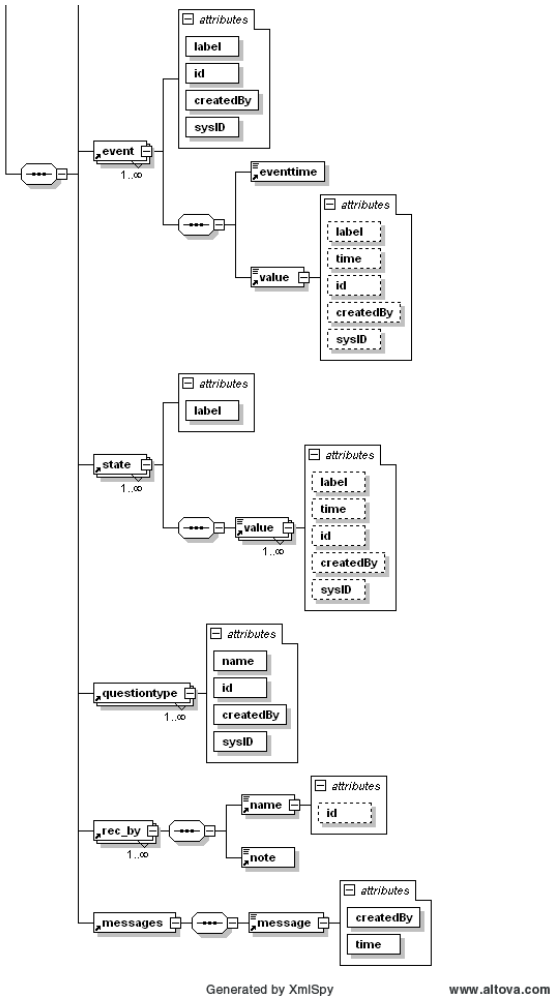


Abbildung D.2.: grafisches Schema der Workflow Struktur - Teil 2

E. Dokumentation und Installation der Simulation

Inhalt der CD

Java Demo GUI	Beinhaltet die das Java Demo GUI Programm
Quelltexte	Hier befinden sich die Quelltexte für die Java Demo GUI und das Businessmodul „firstSim“, das im RFID Anywhere importiert wird
RFIDAnywhere	Beinhaltet die Installationsdateien für RFID Anywhere
RFIDAnywhere Inputs	Die zu importierenden Module für die Simulation in RFID Anywhere
SecondarySources	Enthält die Datei mit den Zusatzinformation für die Kodierung der Tag-IDs
Workfloweditor	Enthält den Workfloweditor zum empfangen der Informationen der Java Demo GUI

Installation RFID Anywhere Die Installation beschränkt sich in diesem Fall auf den Download und die Installation von RFID Anywhere. Die Installationsdateien liegen der CD im Anhang bei. Im Ordner ***RFIDAnywhere*** befinden sich die notwendigen Dateien. Die Installationshinweise entnehmen sie bitte der mitgelieferten Dokumentation.

Nach der erfolgreichen Installation starten sie den RFID Anywhere Service mit einem Klick auf ***Start Service*** im RFID Anywhere Ordner. Anschließend rufen sie Im Internet

Explorer den Pfad `http://localhost/RfidAnywhere/` auf. Nach dem Login mit ihren Anmeldedaten müssen sie nun die von mir erstellten Simulationsbestandteile laden. Dafür klicken sie auf den Reiter Management und wählen da drunter die Option Import. Im nun folgenden Dialog wählen sie die den ***RFIDAnywhere Inputs*** Ordner auf der CD aus und markieren die ***RA Imports.zip*** Datei. Alle anderen Optionen verbleiben bei ihren Standardeinstellungen. Nach einem Klick auf Open werden die Module in die bestehende Konfiguration integriert. Befinden sich die Module

- firstSim
- InvTracAleTCP
- FileOutput
- PatTracSim1
- PatTracSim2
- PatTracSim3
- PatTracSim4

in der Liste der Local Services ist die Installation erfolgreich gewesen.

Nun müssen noch die Zusatzinformationen aktualisiert werden. Unter dem Punkt Local Services klicken sie auf den Eintrag ***firstSim*** in der Liste der Module. Auf der rechten Seite klicken sie nun auf das Plus vor dem Eintrag ***SecondarySourcesXML***. Eventuelle Einträge löschen sie mit einem KLick auf das rote X am Ende des Eintrags. In das leere Feld kopieren sie den Pfad Der ***SecondarySources_FE.XML*** Datei auf der CD. Diese befindet sich im Ordner ***SecondarySources***. Sie können die Datei auch an einer beliebigen anderen Stelle auf ihrem Rechner hinterlegen und den Pfad dahin anschließend in das eben genannte Feld eintragen. Nachdem sie den Pfad + den Dateinamen in das Feld geschrieben oder kopiert haben, klicken sie noch rechts auf das grüne Plus. Nachdem dies erledigt ist, müssen sie zum speichern oben auf die grüne Diskette links neben dem Namen „firstSim“ klicken! Im Anschluss müsste die Seite wie in Abbildung E.1 aussehen:

Das Setup der RFID Anywhere Middleware für die Simulation ist damit abgeschlossen.

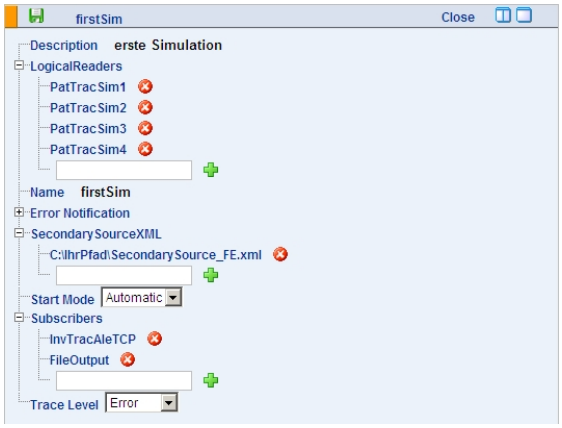


Abbildung E.1.: Einstellungen für die Optionen des Business Moduls „firstSim“

Starten der Simulation Starten sie nun die ***RFID Java Demo.jar***, die sich auf der CD im Verzeichniss ***Java Demo GUI*** befindet. Ein installiertes Java der Version 1.6 vorausgesetzt öffnet sich nun das Fenster der Java Demo GUI.

Jetzt müssen nur noch die RFID Events gestartet werden. Dazu kehren sie zu der RFID Anywhere Administratorkonsole im Internet Explorer zurück. Starten sie nun das Business Modul ***firstSim*** indem sie davor ein Häkchen setzen und oben auf das Zahnrad mit dem grünen Dreieck namens ***Starts selected services*** klicken.

Danach wählen sie ***PatTracSim1, PatTracSim2, PatTracSim3, PatTracSim4*** sowie ***InvTracAleTCP*** aus und klicken wieder auf ***Starts selected services***. Die Simulation der RFID Events läuft jetzt ab. Der Verlauf lässt sich jetzt im Java Demo GUI beobachten.

Nach gut 60 Sekunden endet die Simulation. Die Demo GUI und die Events müssen nun neu gestartet werden für eine Wiederholung der Anzeige.

Workfloweditor Zum starten des Workfloweditors, führen sie im Ordner ***Workfloweditor*** zuerst die Verknüpfung Server aus und dann die Verknüpfung Client. Im öffnenden Clientfenster klicken sie auf die roten Optionen. In den Optionen für den ***Provider web Service*** tragen sie anstelle von „localhost“ ihre aktuelle lokale IP ein. Danach klicken

sie auf ***Connect to Server***. In dem ***Client web Service*** Menü klicken sie lediglich auf ***Start web service***. Nach der Auswahl ***live*** in der ***Generic Configuration*** startet der Editor.

Glossar

DRG Die Diagnosis Related Groups oder übersetzt Diagnosebezogene Fallgruppen, stehen für die Abkürzung DRG. Damit ist ein 2003 eingeführtes Abrechnungssystem gemeint, dass die Behandlung von Patienten anhand ihrer Diagnosen und Behandlung in Fallgruppen einteilt. Diese Fallgruppen werden nach einen festgelegten Betrag vergütet, was das vorherige System der Tagespauschalen ablöst.. 9

Feldemitter Gerät das ein Magnetfeld aussendet um RFID Tags zu aktivieren. Es selbst kann aber keine Informationen lesen.. 33

Kondensator Ein Kondensator ist ein passives elektrisches Bauelement, dass in der Lage ist eine elektrische Ladung und damit Energie zu speichern.. 15

LAN Ist die Abkürzung für Local Area Network und bezeichnet einen Verbund von Rechnern über ein Netzwerk, welches eine geringe Größe besitzt. Dieses umfasst selten mehr als die Größe eines Gebäudes.. 40

Responder Eine technische Einheit, die auf Anfragen antwortet. Im Fall des RFID-Transponders ist der Responder die Einheit, die auf die Anfragen des Lesegerätes reagiert und Nachrichten zurück sendet. . 15

Transmitter Ein Gerät zum Erzeugen und Aussenden von elektromagnetischen Wellen, welche Vorher mit einem sinnvollen Signal moduliert wurde.. 15

Triangulation Sie beschreibt eine Messtechnik zur Ermittlung von Entfernungen. Dabei werden von zwei verschiedenen Punkten, z.B. mit Hilfe von Licht oder elektromagnetischen Wellen, die Entfernung zum Objekt gemessen. Aus der Laufzeit zwischen den Sendern plus den dazu bekannten Winkeln zum Objekt, lässt sich dessen Position errechnen.. 74

URI Der URI ist ein Identifikator, der ein Schema zur Identifizierung von abstrakten oder physischen Ressourcen im Internet bereitstellt. So ist zum Beispiel die Angabe einer Webseite (die URL) auch eine URI mit dem Schema http oder ftp.. 48

Ubiquitous Computing Es beschreibt die dritte Phase der Computerentwicklung, auch das „Internet der Dinge“ genannt. Die Phase, die gerade beginnt, beschreibt die Allgegenwärtigkeit von Rechnern. Sie sind aber nicht mehr sichtbar sondern bestehen aus einem Netzwerk vieler einzelner intelligenter Gegenstände, die im Hintergrund agieren.. 13

WLAN Die Abkürzung für Wireless LAN bezeichnet ein drahtloses lokales Funknetz, in dem ein Rechnerverbund durch Funkübertragung miteinander kommuniziert.. 40

Workflow Der Workflow oder Arbeitsablauf beschreibt eine Abfolge von Aktivitäten in einer definierten Reihenfolge. Er ist die Abbildung eines realen Vorganges, der aus unterschiedlichen Sichten auf den Prozess erfolgt.. 9

Yagi Eine Richtantenne zum Empfang elektromagnetischer Wellen. 33

Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe, insbesondere sind wörtliche oder sinngemäße Zitate als solche gekennzeichnet. Mir ist bekannt, dass Zuwiderhandlung auch nachträglich zur Aberkennung des Abschlusses führen kann.

Ort Datum Unterschrift